Complying with the GDPR When Vulnerable People Use Smart Devices

PhD Thesis

By Stanisław Tadeusz Piasecki

Thesis submitted to the University of Nottingham for the degree of Doctor of Philosophy
July 2022

Abstract

The number of smart home devices is increasing. They are used by vulnerable people regardless of whether they are designed specifically for them or for the general population (for example, smart door locks, smart alarms or voice assistants). This PhD focusses on children and inherently vulnerable adults, and analyses how to comply with the General Data Protection Regulation (GDPR) when the latter use smart products, with a particular focus on the UK through references made to the Information Commissioner's Office guidelines and reports. Complying with the GDPR provisions related to the processing of vulnerable people's data would be beneficial not only for the latter but also for organisations developing and deploying smart devices. This thesis argues in favour of protecting vulnerable people's data by design and default in every smart product. The objective of this work is also to draw attention to the need of thinking about vulnerability across all data protection principles and to propose solutions on how to effectively comply with the GDPR in this context.

This PhD contains a legal doctrinal chapter, an empirical part (interviewing lawyers and technologists working within the smart home field) as well as a chapter related to theoretical debates and privacy enhancing technologies (PETs).

In the doctrinal chapter, research into data protection law and legal concepts is conducted to understand the current legal landscape, guidelines and opinions related to this field of study. Personal data can be processed only if an appropriate legal basis is chosen and all of its conditions are met, and if all GDPR principles are respected. In this part of the thesis, the most relevant data protection law provisions in the context of the use of smart products by vulnerable people are identified and discussed.

The empirical chapter introduces information gathered through semi-structured interviews conducted with UK and international professionals in the field of data protection law and technology design, with a focus on the smart home context. Those discussions gave various insights and perspectives into how the two communities view intricate practical data protection challenges.

The chapter related to theoretical debates and PETs analyses personal information management systems (PIMS) in order to understand how to protect and manage vulnerable people's data more effectively in smart homes and, as a result, enhance compliance with data protection law. Relying on PETs to safeguard vulnerable people's personal data could lead to questions as to the normative grounds for this technological approach. By examining debates such as privacy-as-confidentiality versus privacy-as-control, this thesis explains why edge computing PIMS could help in improving GDPR compliance while underlining that designers of PIMS need to consider the consequences of implementing different privacy paradigms.

Keywords

Data protection law; compliance; internet of things; smart devices; vulnerable people; children; privacy enhancing technologies; personal information management systems

Acknowledgements

I would like to sincerely thank all the great people who have supported me during this PhD journey.

Firstly, I would like to offer my gratitude to my supervisors Prof Derek McAuley, Dr Jiahong Chen and Prof Elvira Perez Vallejos, for all their invaluable advice, support and mentorship.

To Prof Hiroshi Miyashita, for kindly welcoming me as Visiting Researcher at Chuo University in Tokyo, for his guidance and all the opportunities that he gave me during my stay.

To all those who have guided me throughout my time as a PhD student, in particular Prof Richard Hyde, Dr Lachlan Urquhart, Dr Dimitri Darzentas, Prof Steve Benford and Ms Kate Duncan.

I am honoured and grateful to have met all of you.

To all my interview participants, who offered me their time and insights.

To the UK Engineering and Physical Sciences Research Council and the Horizon Centre for Doctoral Training for funding this research.

To all the students of the Horizon CDT 2018 cohort for all the great moments we have shared together.

To all my friends from outside academia, for their presence, honesty and strength that they have given me throughout the years.

To my family, and especially my parents. Thank you for your love, patience and support.

Stanislaw Tadeusz Piasecki

July 2022

Table of Contents

Abbreviations

CJEU – Court of Justice of the European Union

DCMS – Department for Digital, Culture, Media and Sport

DPA – Data Protection Authority

DPbDD – Data Protection by Design and by Default

DPIA – Data Protection Impact Assessment

ECtHR – European Court of Human Rights

EDPB – European Data Protection Board

EDPS – European Data Protection Supervisor

ENISA – European Union Agency for Network and Information Security

GDPR – General Data Protection Regulation

HRESIA – Human Rights, Ethical and Social Impact Assessment

ICO – Information Commissioner's Office

IEEE – Institute of Electrical and Electronic Engineers

IoT – Internet of Things

ISS – Information Society Services

PET – Privacy Enhancing Technology

PIMS – Personal Information Management Systems

TA – Thematic Analysis

WP29 – Article 29 Data Protection Working Party

Chapter 1: Introduction

The introductory chapter explains the PhD's objectives (Section 1.1). Subsequently, it discusses why protecting vulnerable people's personal data is particularly important in the smart home context, who is defined as vulnerable for the purpose of this thesis as well as the structure and methods adopted in this study (Section 1.2).

Section 1.1 Objectives of this Study

This PhD critically analyses how compliance with the General Data Protection Regulation (hereinafter 'GDPR') works in theory and in practice from the perspective of organisations developing and deploying smart devices used (or that could be used) by vulnerable people.[1] Firstly, a doctrinal study evaluates how the law is written and interpreted by researchers, regulators, judges and institutions in this particular context. The objective of this part of the PhD is to draw attention to the need of thinking about vulnerability across all data protection principles and to protect vulnerable people's data by design and by default in every smart product. Secondly, this thesis analyses how these topics are viewed by professionals (lawyers and technologists). Subsequently, it evaluates privacy enhancing technologies (personal information management systems in particular) as potential technical solutions to data protection compliance issues. Theoretical debates are also discussed to explain the normative grounds for this technological approach.

It is worth briefly noting that the GDPR still applies in the UK (with the caveat that it has independence to modify the framework in the future) as it has been incorporated into national legislation under the name of UK GDPR and that, in any case, organisations processing EU residents' data still need to comply with the EU GDPR.[2] This study focusses on inherently vulnerable adults and children. Complying with the GDPR requirements related to the processing of vulnerable people's data would be beneficial not only for the latter but also for organisations developing and deploying smart products. As this chapter will discuss in more

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation, 'GDPR'), [2016] OJ L 119/1.

[2] Information Commissioner's Office, 'The UK GDPR' (2022) <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/> accessed 1 July 2022.

detail, companies could potentially avoid fines, business disruption and gain trust of their customers by protecting vulnerable people's rights. Smart home devices are used by vulnerable individuals regardless of whether they are designed specifically for them or for the general population (for example, smart door locks, smart alarms or voice assistants). The GDPR has various provisions related to vulnerability and organisations need to comply with them (this will be analysed in-depth in Chapter 2). For example, Art. 6.1 (f) GDPR requires organisations to be particularly strict when balancing their legitimate interests against those of a child. Some of the special measures adopted for vulnerable persons could be beneficial for all people (for example, writing privacy policies in a child-friendly language) while others would need to be adapted to the needs of particular groups of vulnerable individuals (for example, in the case of smart devices sold to people living with dementia). Informational privacy is essential to the recognition of children and vulnerable adults as people whose dignity is protected.[3] Apart from international treaties such as the United Nations Convention on the Rights of the Child, the GDPR also recognises an inherent link between informational privacy and human dignity in its Art. 88.[4] What are the particularities of data protection law compliance when vulnerable individuals use smart home products? What kind of measures should organisations take to comply with the GDPR when their smart devices are used by vulnerable people? On which GDPR principles should they focus? This PhD evaluates what it considers as the most relevant GDPR provisions to the rights and freedoms of vulnerable individuals.

This thesis identifies pertinent issues and provides potential solutions based on a legal, empirical and technological analysis. The PhD raises awareness about current problems with data protection compliance so that they can be discussed by researchers and resolved by policy makers. Moreover, if organisations have the capacity, incentive and knowledge to comply with GDPR provisions, this would increase the availability, quality and security of smart products offered to vulnerable persons (and their legal guardians). This study will help organisations with legal compliance and, as a result, enhance the protection of vulnerable adults' and children's data and rights.

[3] J. C. Buitelaar, 'Child's Best Interest and Informational Self-Determination: What the GDPR can Learn from Children's Rights' (2018) 8(4) International Data Privacy Law 293.
[4] Convention on the Rights of the Child, GA Res. 44/25, annex, 44 UN GAOR Supp. (No 49) at 167, UN Doc. A/44/49 (1989).

Section 1.2 Background: Data Protection Compliance and Smart Homes

This PhD firstly briefly defines personal data (1.2.I), vulnerable persons (1.2.II) and smart homes (1.2.III). The latter are becoming increasingly insecure environments because of the situational and informational harms they create while risks of fines, negative business reputation and disruption are looming on organisations developing and deploying smart devices (1.2.IV). An overview of the methods and structure of this thesis is also provided in this section (1.2.V).

1.2.I Blurred Line Between Personal and Non-Personal Data

The first important issue to mention is that the line between personal and non-personal data can be blurred, and data currently considered as non-personal can become personal in the future, for example, due to technological progress allowing reidentification. As a result, analysing the conceptual boundaries of personal data has to come before exploring the topic of vulnerable people's data protection. In the GDPR, personal data is defined as 'any information relating to an identified or identifiable natural person ("data subject")'.[5] The fact that a particular piece of data can be analysed in unlimited ways raises the issue of the possibility that any data collected in smart homes could eventually lead to the identification of an individual and divulge sensitive information. Data points can be construed as presenting both non-personal and personal information depending on the context of the processing, which leads according to some to the disappearance of the distinction between personal and non-personal data.[6] On the other hand, others could argue that non-personal data does exist if it does not lead to the identification of an individual at a particular moment in time. Data can be anonymised using different techniques such as differential privacy.[7] These processes can be more or less effective. In light of these considerations and in the specific context of vulnerable individuals, this thesis does not differentiate between personal and non-personal data, adopting the view that any data originating from a vulnerable person should be considered as potentially personal. Some vulnerable data subjects might not be aware that a certain kind of data could be

[5] GDPR, art 4.

[6] Nadezhda Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn?: Individual Control and Transparency' (2017) 10(2) Journal of Law and Economic Regulation 64.

[7] The Royal Society, 'Protecting Privacy in Practice. The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis' (March 2019) <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf> accessed 1 July 2022 49-50.

reidentified in particular circumstances or that, for example, their metadata gathered by smart products can be used to analyse their patterns of behaviour within their private homes and identify them for various purposes. This interpretation is in line with the GDPR as it mandates the adoption of special protective measures in relation to vulnerable people's personal data. This thesis will now analyse those provisions and explain how it defines vulnerability for the purposes of this study.

1.2.II Defining Vulnerable Individuals

According to the United Nations Convention on the Rights of the Child (ratified by the UK), a child means anyone under the age of 18, unless 'under the law applicable to the child, majority is attained earlier'[8]. In the UK, majority is attained at the age of 18 years old. Art. 8 GDPR states that the parental consent mechanism generally applies when the child is younger than 16. Processing personal data will be lawful only if the child's parent or custodian has consented to such processing.[9] However, Member States are allowed to lower this threshold in national legislation up to 13 years old, which has been done in the UK. Children are the only group of vulnerable people that is explicitly mentioned in the GDPR (Rec. 38, Rec. 58, Rec. 65, Rec. 71, Rec. 75, Art. 6.1 (f), Art. 8, Art. 12, Art. 40.2 (g) and Art. 57.1 (b)) and the only time that the term vulnerability appears is in Rec. 75, which states that 'the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage', especially 'where personal data of vulnerable natural persons, in particular of children, are processed' (it should be noted that while recitals can help in the interpretation of ambiguous EU law provisions, they are not legally binding). The GDPR therefore places emphasis on children as requiring particular attention while not excluding other categories of vulnerable people, just not mentioning any explicitly. Rec. 38 of the GDPR states that children's personal data requires special protection measures to be taken by the data controller as they 'may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'. This should be also true for other groups of vulnerable people for whom such specific measures should be taken as well. This approach is in conformity with other European

[8] Convention on the Rights of the Child art 1 (n 4).

[9] Christina Tikkinen-Piri, Anna Rohunen and Jouni Markkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' (2018) 34(1) Computer Law & Security Review 134, 138.

Union (EU) data protection legislation, such as Directive 2016/680, which states in Rec. 39 that any information provided to the data subject 'should be adapted to the needs of vulnerable persons such as children'.[10]

As to the definition of vulnerability, the UK's Information Commissioner's Office (ICO) informs that 'individuals can be vulnerable where circumstances may restrict their ability to freely consent or to object to the processing of their personal data, or to understand its implications'.[11] This is a very broad definition of vulnerability, encompassing a wide array of situations. This shows that ICO's objective is to cover all kinds of vulnerabilities when it comes to data protection. Concerning vulnerable adults, the ICO gives examples of older people or those living with particular disabilities while not giving a definitive list. It states that even in the case where someone cannot be automatically categorised as vulnerable, a power imbalance in their relationship with another person can create a situation of vulnerability in the context of the GDPR. An example of this are employees who can be treated as vulnerable when there is a power imbalance as a result of which they have difficulties to object to the processing of their personal data by their employer.[12] The ICO adds that this kind of vulnerability can also arise in other circumstances, for example, in relation to an individual's financial situation (when establishing a credit rating etc.) or when a patient's data is being processed for medical care reasons.[13]

On the EU level, the Article 29 Data Protection Working Party (WP29) stated that vulnerable data subjects can include employees, children (because they can be considered as not having the capacity to consciously and thoughtfully consent or oppose data processing activities), vulnerable groups of the population needing special protection (people with mental health problems, the elderly, patients etc.), and in any situation in which an imbalance of power

[10] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive, 'LED'), [2016] OJ L119.

[11] Information Commissioner's Office, 'When do we need to do a DPIA?' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/> accessed 1 July 2022.

[12] Article 29 Working Party, 'Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679' (WP 248, 4 October 2017).

[13] Information Commissioner's Office, 'When do we need to do a DPIA?' (n 11).

between the controller and the data subject exists.[14] This is a large definition and non-exhaustive list of vulnerable individuals, similar to ICO's guidelines. In 2016, the European Parliament has published a report related to what it considers as the only legislative instrument that might be effective in improving the protection of vulnerable adults in cross-border situations – the Hague Protection of Adults Convention.[15] Even though this convention deals specifically with vulnerable adults, it does not provide a definitive definition of who they are. It only informs that it 'applies to the protection in international situations of adults who, by reason of an impairment or insufficiency of their personal faculties, are not in a position to protect their interests' (Art. 1).[16]

An attempt to categorise vulnerable people can also be found in UK's national legislation, namely in the Safeguarding Vulnerable Groups Act 2006. In Schedule 4, the Act provides a list of circumstances in which a person is considered as a vulnerable adult. For example, adults over 18 are vulnerable when they are receiving domiciliary care or any form of health care and if they require assistance in the conduct of their own affairs.[17] Those conditions also encompass a large variety of factual situations and are framed widely.

Vulnerability conveys a large diversity of fact-based situations – from adults who are under the umbrella of court-appointed guardianship to instances when an older person is just not able to perform certain actions as a consequence of old age, independently from their mental capacity. The wide range of mental and physical conditions that are relevant requires a flexible approach. Anyone can become vulnerable under particular circumstances. Legislation and relevant actors should be responsive and adaptive when this happens. The approach of the European Court of Human Rights (ECtHR) reflects this as it builds an ever-expanding case law on existing and emerging groups of vulnerable people. This can help in the mission to achieve a more 'robust idea of equality'.[18]

[14] Article 29 Working Party 'Guidelines on Data Protection Impact Assessment (DPIA)' (n 12).

[15] Christian Salm, 'Protection of Vulnerable Adults' (*European Parliament, European Parliamentary Research Service*, September 2016) <https://www.europarl.europa.eu/RegData/etudes/STUD/2016/581388/EPRS_STU(2016)581388_EN.pdf> accessed 1 July 2022; Convention on the International Protection of Adults, The Hague, UN, Treaty Series, vol. 2600, at 3 (2000).

[16] Ibid.

[17] Safeguarding Vulnerable Groups Act 2006 (UK).

[18] Oddný Mjöll Arnardóttir, 'Vulnerability under Article 14 of the European Convention on Human Rights' (2017) 1(3) Oslo Law Review 150; Lourdes Peroni and Alexandra Timmer, 'Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention law' (2013) 11(4) International Journal of Constitutional Law 1056, 1074.

While vulnerability has been rarely explored by privacy and data protection researchers, Malgieri and Niklas recently analysed 'the role and potentiality of the notion of vulnerable data subjects'.[19] They stated that vulnerability can be viewed as universal (all individuals are equally vulnerable) or particular (some individuals are more vulnerable than others). Indeed, researchers have previously argued in favour of both. According to Fineman, vulnerability is a universal element of the human condition and shared by all while Cooper underlines that while this may be true, a universal approach conceals the specific experiences based on identities, such as those of young men of colour who 'continue to be always already suspect to the police'.[20] Malgieri and Niklas consider that 'situating vulnerability in the data protection framework is a problematic task' because if all data subjects are considered universally vulnerable, then important differences between them could be ignored (thereby exacerbating the already disadvantageous position of some persons), while making data protection rules and safeguards more specific could result, among other issues, in the fragmentation of an already complex legal landscape.[21] As a solution to this conundrum, they propose Luna's theory of layered vulnerability.[22] Luna overcomes the universal versus particular divide by arguing that all people are vulnerable but that some persons possess more vulnerability layers than others. This layered approach seems to reflect GDPR's risk-based approach, the latter suggesting that anyone can be vulnerable but at various levels and in different contexts. It also reflects Calo's stance that 'no one is entirely invulnerable at all times and in all contexts' and that 'we are all vulnerable in degrees and according to circumstance'.[23] Calo argues that while the law usually considers vulnerability as a status of a person or group or as a relationship between individuals and organisations, legal research increasingly acknowledges that this concept is best perceived as 'layer of personhood', a condition that exists more frequently and intensively in some individuals and contexts, but in all people sometimes.[24] How does this debate translate into the contribution that this PhD is trying to make in the data protection field?

[19] Gianclaudio Malgieri and Jędrzej Niklas, 'Vulnerable Data Subjects' (2020) 37 Computer Law & Security Review 105415.

[20] Martha Albertson Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2008) 20(1) Yale Journal of Law and Feminism 1; Frank Rudy Cooper, 'Always Already Suspect: Revising Vulnerability Theory' (2015) 93(5) North Carolina Law Review 1339, 1379.

[21] Malgieri and Niklas 5 (n 19).

[22] Florencia Luna, 'Elucidating the Concept of Vulnerability: Layers Not Labels' (2009) 2(1) International Journal of Feminist Approaches to Bioethics 121.

[23] Ryan Calo, 'Privacy, Vulnerability, and Affordance' (2017) 66(2) The De Paul Law Review 591, 593.

[24] Ibid.

This study agrees that layers of vulnerability can manifest in any person and that the layered approach has the benefit of taking everyone into consideration, even the most subtle cases of vulnerability, while also promoting an intersectional and cumulative approach. However, it also argues that in some situations, categorising vulnerable individuals can be helpful to ensure a higher level of their data protection. This thesis does not focus on 'contextual' vulnerability but rather on children and adults who are considered inherently vulnerable, that is whose layers of vulnerability are constantly and unequivocally present, such as adults with cognitive disabilities. Children 'have limited capacity to understand the complexity of data-driven architecture, have less experience, less awareness of risks and rights and may be easily manipulated' (this is reflected in GDPR's provisions) while the inherent vulnerability of adults with cognitive disabilities has been confirmed in the case law of the ECtHR.[25] There are many vulnerability layers or other situations in which people could be considered as vulnerable (for example, the above-mentioned situations of imbalance of power between employers and employees) but deciding whether they actually are would require a case by case analysis. Those subtle vulnerabilities do not fall into the scope of this work. Such a choice of focus has the benefit of highlighting the most pressing practical challenges with less distractions from borderline cases. Of course, this does not mean that the latter are less important in any way, but as a first research attempt in this field, this study chooses to focus on inherently vulnerable individuals to highlight the importance of reflecting on vulnerability when applying the GDPR to a smart home context.

A problem that can arise from the fact that the GDPR only mentions one group of vulnerable people (children) explicitly, is that organisations might focus on the latter while ignoring other types of vulnerabilities. Vulnerable adults are certainly protected by European data protection laws but vulnerability could be viewed as too much of an abstract concept for those working on smart products to adjust their data protection measures effectively. Some organisations could view the lack of guidance in the GDPR as an indication that there is no need to dedicate as many resources to protect vulnerable adults as in the case of children. For this reason, guidelines of European and national data protection authorities on how to implement the GDPR are particularly important. However, the adoption of the Age Appropriate Design code of

[25] Alexandra Timmer, 'Vulnerability: Reflections on a New Ethical Foundation for Law and Politics' in Martha Albertson Fineman and Anna Grear (eds), *A Quiet Revolution: Vulnerability in the European Court of Human Rights* (Ashgate 2013); Alexandra Timmer, 'Strengthening the Equality Analysis of the European Court of Human Rights: The Potential of the Concepts of Stereotyping and Vulnerability' (Doctor of Law, Universiteit Gent 2014); Malgieri and Niklas (n 19).

practice by the UK's Information Commissioner's Office is another indication that both data protection authorities and data controllers have focussed on the case of children.[26] If a data controller considers that its product will not be used by children (although as we will argue later, it is better to assume that it always could), this could undermine vulnerable adults' data protection as the controller might ignore or lack knowledge on the special data protection measures it should adopt. One solution to this problem could be Art. 40 of the GDPR which states that the Commission, through implementing acts, can decide that a code of conduct has 'general validity within the Union'. If a code of conduct discussing vulnerable adults was written, the Commission could promote its application in all Member States.

In summary, the GDPR does mention vulnerable people and discusses special measures that need to be adopted by organisations, especially in relation to children. While there is no definitive list of situations in which an adult should be considered as vulnerable, organisations working on smart devices are required by the GDPR to adapt their data protection compliance policies to take into consideration vulnerable people's needs. They are certainly required to do so if their products are being used by inherently vulnerable individuals such as adults with cognitive disabilities and children.

1.2.III Significant Data Protection Issues Associated with Smart Homes

What are smart homes and why should we concentrate on this particular setting? A smart home may be defined as 'a contemporary application of ubiquitous computing that incorporates intelligence into dwellings management for comfort, healthcare, safety, security, and energy conservation'.[27] A truly smart home is one where 'all data about the environment is collectively stored and analysed, patterns extracted, and decisions made without the user's intervention'.[28] Any device could become smart and used within people's homes. Some categories of smart home-related products are smart safety devices such as door locks, security cameras or smoke detectors; home automation and smart alarm systems; entertainment devices such as smart TVs or speakers; smart home assistants such as Alexa, Siri, Cortana or Google Home; smart appliances such as washing machines, fridges, kettles or light bulbs. These devices are also

[26] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (2 September 2021) <https://ico.org.uk/for-organisations/childrens-code-hub/> accessed 1 July 2022.
[27] Dragos Mocrii, Yuxiang Chen and Petr Musilek, 'IoT-Based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security' (2018) 1-2 Internet of Things 81, 81.
[28] Ibid.

often called Internet of Things (IoT) products or connected consumer products. The Institute of Electrical and Electronics Engineers (IEEE) has attempted to create an all-inclusive definition of what IoT is.[29] In order to do so, it has mapped state of the art definitions provided by standardisation organisations, academics and many other sources. The IEEE concluded that 'An IoT is a network that connects uniquely identifiable 'Things' to the Internet. The 'Things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the 'Thing' can be collected and the state of the 'Thing' can be changed from anywhere, anytime, by anything'.[30] In this work, the terms smart devices and IoT products will be used interchangeably.

The omnipresence of smart products is becoming a reality in many countries and their further increase in numbers globally seems certain in the longer term. According to current reports, there will be 21.5 billion IoT devices and 25% more cyber-attacks by 2025 (compared to 7 billion devices in 2018).[31] Smart devices are transmitting increasing amounts of data across the internet. They often collect personal data and transfer such data to the cloud for analysis. The results are integrated back into the device to make services more effective. For example, organisations can gain knowledge about voice patterns and people's preferences by analysing data gathered through smart speakers.[32] Data hacks related to IoT products are likely to rise in numbers, to a certain degree because of poor security measures (such as default passwords not being modified) and cloud-architectures that lead to the current mining of data, storage in cloud databases and various data privacy threats associated with it.[33] The scale of recent data breaches shows that this is likely to happen.[34]

Consumers are rarely conscious of the risks to their data when they use smart products and do not possess technical capacities to set up a safe smart home environment.[35] They frequently

[29] IEEE, 'Towards a Definition of the Internet of Things (IoT)' (27 May 2015) 74 <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf> accessed 1 July 2022.

[30] Ibid.

[31] Knud Lasse Lueth, 'State of the IoT 2018: Number of IoT Devices now at 7B – Market Accelerating' (*IoT Analytics,*, 8 August 2018) <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/> accessed 1 July 2022.

[32] Lachlan Urquhart, Holger Schnädelbach and Nils Jäger, 'Adaptive Architecture: Regulating Human Building Interaction' (2019) 33(1) International Review of Law, Computers & Technology 3.

[33] Stanislaw Piasecki, Lachlan Urquhart and Derek McAuley, 'Defence Against the Dark Artefacts: Smart Home Cybercrimes and Cybersecurity Standards' (2021) 42 Computer Law & Security Review 105542.

[34] Gartner, 'Leading the IoT: Gartner Insights on How to Lead in a Connected World' (2017) 13 <https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf> accessed 1 July 2022.

[35] Karlijn van den Heuvel, 'Securing the Smart Home' (Masters thesis, University of Amsterdam 2018).

have problems with device management as well as network management. As a consequence, smart devices should be given special attention by policy makers as well as those developing and deploying them. People will be able to effectively manage their devices and networks (and therefore protect their data) only if this is made easy for them.[36]

Threats linked to IoT home products are not a recent problem and some are well-known for a long time now. Already in 2014, the Article 29 Data Protection Working Party had recognised the existence of various threats to personal data security arising from smart devices.[37] Those threats are related to consumers being monitored by third parties and not having real control over how their personal data is exploited. Other risks concern modifying the purpose of processing people's data, profiling techniques and gaining information about users' behaviour patterns. Staying anonymous has become increasingly difficult for people who own IoT devices within their homes.[38] People can also be victims of identity theft, cyber harassment and discrimination, and have their reputation tarnished because of leaks and takeovers of data. Moreover, cybercriminals do not stop inventing new threats and they are often successful in overcoming security barriers. Vulnerable people may have lower capacities to defend themselves against such data security risks. The GDPR recognises that there is a need to adapt data protection mechanisms to vulnerable people's situations (for example, Rec. 38 and Rec. 75 GDPR).

New technologies have been used to help vulnerable individuals in various ways for a long time now. People with different health conditions or simply experiencing symptoms associated with old age have been able to live more autonomously as a result of technological advances. This has been the subject of a longstanding line of research in computing under the heading of ambient assisted living. The use of smart devices is just the latest development in this field. Exploring how those products process vulnerable people's data is crucial. Vulnerability can have consequences either during data processing (for example, there may be more risks for some persons in terms of providing informed consent) or as a result of the processing (data processing could lead to discrimination or, for example, psychological harms).[39] Among smart

[36] Anne Adams and Martina Angela Sasse, 'Users are Not the Enemy' (1999) 42(12) Commun Acm 40.

[37] Article 29 Working Party, 'Opinion 8/2014 on the recent developments on the Internet of Things' (WP 223, 16 September 2004).

[38] Ibid.

[39] Malgieri and Niklas (n 19).

devices, some of them are targeting specific categories of individuals.[40] In the case of children, new internet-connected toys have been appearing on the shelves of shops such as interactive dolls or robots.[41] Parents also purchase products such as smart baby monitors or smart watches that track their child's sleep patterns, location and medical data.[42] In the case of people living with dementia, there are many health devices or tracking devices developed to support them in their daily activities.[43] IoT products targeting specific parts of the population require a more focussed approach from data controllers based on the consumers' specific layers of vulnerability (and on data protection impact assessments that organisations should conduct in this context) as this could help in ensuring that measures are better adapted to their needs at the data processing stage. Widely used devices, such as voice assistants, are more difficult to adapt to everyone as everyone's layers of vulnerability are different. This could be partly tackled by preventing potential negative effects of data processing through more general data protection safeguards (implementing the data protection by design and by default principle), which will be explored later in this thesis.

As a consequence of the rapid expansion of the IoT world and the fact that an increasing number of people will live within smart homes over time, it is crucial to discuss how to best protect personal data of those who are the most vulnerable. Because of the way most IoT devices are currently designed, as their number increases, the number of security issues will unfortunately most probably rise as well. It is important to implement data protection provisions in a way that protects vulnerable users against potential breaches and helps them in deciding how their data is processed. Calls for special data protection measures in relation to children's activities online and to transform their fundamental rights to privacy established in Art. 16 of the United Nations Convention on the Rights of the Child have resulted in new GDPR provisions on vulnerability in comparison to previous EU legislation.[44] This means

[40] Brent Arnold and Kavi Sivasothy, 'He Sees You when You're Sleeping, He Knows When You're Awake: Smart Toys and Regulating the IoT in Canada' (*Gowling WLG*, 17 December 2018) <https://gowlingwlg.com/en/insights-resources/articles/2018/smart-toys-and-regulating-the-iot-in-canada/> accessed 1 July 2022.

[41] Lisa Collingwood, 'Villain or Guardian? 'The Smart Toy is Watching You Now … .'' 30(1) Information & Communications Technology Law 75, 75.

[42] Ingrida Milkaite and Eva Lievens, 'Child-Friendly Transparency of Data Processing in the EU: from Legal Requirements to Platform Policies' (2019) 14(1) Journal of Children and Media 5.

[43] Sarah Palmdorf and others, 'Technology-Assisted Home Care for People With Dementia and Their Relatives: Scoping Review' (2021) 4(1) JMIR Aging e25307.

[44] Milda Macenaite, 'From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation' (2017) 19(5) New Media & Society 765; Convention on the Rights of the Child (n 4).

organisations need to adapt their data protection policies to children's and other vulnerable people's needs. For organisations, being compliant with data protection regulations is not only a matter of avoiding monetary sanctions but can also be a strategic move to gain customers' trust.

1.2.IV Tight Regulations, Business Reputation and Potential Disruption

Complying with data protection regulations is important from the point of view of the economic interests of organisations working on smart devices. If they do not comply with those provisions, they could face severe fines. Indeed, Art. 77 to 84 of the GDPR set out remedies, liabilities and penalties for violations of data protection rules. The GDPR gives to the data subject the right to bring charges against a controller or processor to a supervisory authority and to receive a judicial remedy if their rights are infringed. Supervisory authorities are allowed to impose fines for the infringement of the GDPR up to certain maximum amounts, depending on the context of a particular case. For example, the violation of data protection principles can result in a fine up to €20 million or 4% of the total annual global turnover (whichever is higher). Controllers and processors can be also affected by other fines of varying magnitude depending on the circumstances, such as when they infringe data subjects' rights or fail to keep written records of their processing activities as demanded by the GDPR.[45]

In 2020, the UK's data protection authority (the ICO) fined Marriott International (£18.4 million) and British Airways (£20 million) for revealing their customers' personal data and violating the GDPR.[46] In continental Europe, a technology giant, Google, was fined in 2019 (£50 million) by the French National Data Protection Commission for insufficient transparency and lack of valid consent in relation to its advertisement practices under the GDPR[47]. In the context of vulnerable individuals, a class action lawsuit was lodged against YouTube (it was served on the defendant on 29 July 2020) seeking damages of more than £2.5 billion due to the

[45] Tikkinen-Piri, Rohunen and Markkula (n 9).

[46] Information Commissioner's Office, 'ICO Fines British Airways £20m for Data Breach Affecting more than 400,000 Customers' (16 October 2020) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/> accessed 1 July 2022; BCL Solicitors LLP, '£18.4 Million Marriot International GDPR Fine Announced by IPO: What Did we Learn?' (2 December 2020) <https://www.lawyer-monthly.com/2020/11/18-4-million-marriott-international-gdpr-fine-announced-by-ipo-what-did-we-learn/> accessed 1 July 2022.

[47] Cécile Martin, 'Personal Data: French Data Protection Authority Levies €50 Million Fine (*Ogletree Deakins*, 18 February 2019) <https://ogletree.com/insights/personal-data-french-data-protection-authority-levies-e50-million-fine/> accessed 1 July 2022.

illegal use and collection of children's data for targeted advertising. These are just a couple of examples showing that GDPR infringement can lead to enforcement and potential financial penalties of substantial magnitude.[48]

The GDPR gives incentives to implement its provisions and many organisations have invested funds to enhance their compliance with data protection rules. Being compliant with data protection regulations is not only a matter of avoiding monetary sanctions, but can also be a strategic move to gain customers' trust. Much of the media's focus has been on fines for non-compliance but the effect on business reputation and continuity could be much higher over time.[49] The creation of processes and safeguards that increase consumers' trust is crucial.[50] The actions of two big tech giants prove this. When the California Consumer Privacy Act (now the California Privacy Rights Act) was entering into force, Twitter announced that it will apply its privacy standard globally, not because it needs to but because it's part of a bigger strategy to gain trust of consumers. Similarly, Microsoft announced that it will apply CCPA's provisions in all of the United States.[51] Companies looking into the future think of data protection as a competitive advantage. However, this will not necessarily be the case for less visible issues such as the protection of vulnerable adults' data. To ensure companies implement a truly vulnerability-aware approach, the previously-mentioned enforcement mechanisms seem particularly important.

Not complying with the GDPR could also cause business disruption.[52] If legal action is taken against an organisation and the latter has not been properly managing consumers' data, or did not inform its customers of a data breach, it will be required to go through the process of providing all relevant information and transmitting it as quickly as possible to an investigating

[48] Foxglove, 'YouTube Data Breach Claim' (14 September 2020) <https://www.foxglove.org.uk/2020/09/14/youtube-is-breaking-the-law-by-harvesting-childrens-data-for-targeted-advertising-our-work-to-stop-them/> accessed 1 July 2022; Duncan McCann and others, 'YouTube Data Breach Claim' (2022) <https://www.youtubedataclaim.co.uk/> accessed 1 July 2022; Natasha Lomas, 'YouTube Hit with UK Class Action Style Suit Seeking $3BN+ for 'Unlawful' Use of Kids' Data' (*TechCrunch+*, 14 September 2020) <https://techcrunch.com/2020/09/14/youtube-hit-with-uk-class-action-style-suit-seeking-3bn-for-unlawful-use-of-kids-data/> accessed 1 July 2022.

[49] Joe Garber, 'GDPR – Compliance Nightmare or Business Opportunity?' (2018) 2018(6) Computer Fraud & Security 14.

[50] Timothy Morey, Theodore Forbath and Allison Schoop, 'Customer Data: Designing for Transparency and Trust' (2015) 93(5) Harvard Business Review 96; Garber.

[51] Cillian Kieran Ethyca, 'Twitter and Microsoft show Data Privacy is Moving from Sticking Point to Selling Point' (*VB*, 21 December 2019) <https://venturebeat.com/2019/12/21/twitter-and-microsoft-show-data-privacy-is-moving-from-sticking-point-to-selling-point/> accessed 1 July 2022.

[52] Garber (n 49).

team. If this organisation does not have a good overview of the data it possesses, this could cause high disruption in many of its departments and to its operations in general. It could be even ordered to stop processing personal data (Art. 58 GDPR).

1.2.V Research Methods and Structure of this Thesis

This chapter has presented the PhD topic and explained its importance both for the data controller and the vulnerable data subject. Smart homes are increasingly popular but also insecure spaces for vulnerable people's personal data. Organisations should strive to comply with legislation not only because they risk fines but also because of their business reputation and the disruption that poor data management could cause. This thesis focusses on inherently vulnerable adults and children.

In the second chapter of the thesis, doctrinal research into data protection law and legal concepts is conducted to understand the current legal landscape, guidelines and opinions related to this field of study. Doctrinal legal research 'provides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty and, perhaps, predicts future developments'.[53] A doctrine 'explains, makes coherent or justifies a segment of the law as part of a larger system of law. Doctrines can be more or less abstract, binding or non-binding'.[54] In the doctrinal study, the most relevant data protection law provisions in the context of the use of smart products by vulnerable people are identified and discussed. Smart devices gather, process and transfer high volumes and different types of personal data. This study focusses on the GDPR, an essential governance framework for the development and deployment of smart home systems.[55]

The third chapter of this PhD is the empirical part. The dichotomy that is sometimes observed between doctrinal studies and how laws work in practice has been the subject of criticism by modern legal scholars.[56] The epistemological assumption, methodology, methods and the process of data analysis are described in more detail at the beginning of the empirical chapter.

[53] Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17(1) Deakin Law Review 83, 101.

[54] Trischa Mann, *Australian Law Dictionary* (OUP Australia & New Zealand 7 January 2020).

[55] Sandra Wachter, 'The GDPR and the Internet of Things: A Three-Step Transparency Model' (2018) 10(2) Law, Innovation and Technology 266.

[56] Hutchinson and Duncan (n 53).

In this paragraph, the thesis provides a general overview of its content and methods that have been used. Semi-structured interviews with members of organisations (lawyers and technologists) developing and deploying smart products used by vulnerable people were conducted. Those interviews helped in understanding how data protection laws work in practice and how organisations try to adapt to the current legislation. The variety of interviewees allowed to compare different perspectives and approaches to data protection compliance topics. Answers to the following questions were provided:

- When organisations develop and/or deploy smart devices that use personal data, do they take into consideration the needs of vulnerable groups of people to comply with the GDPR?
- What are the underlying issues linked to the practical data protection law-related challenges faced by organisations working on smart devices used by vulnerable persons?
- How do experts perceive data protection-related problems in this context?

This study addresses GDPR compliance from the perspective of organisations developing and deploying smart home products. It focusses on the views of professionals working for those organisations. Views of other stakeholders (such as vulnerable individuals themselves, parents or medical professionals) are not included in this thesis. This choice will be also further explained in the beginning of the third chapter.

Finally, the last chapter analyses how the relationship between IoT products, vulnerable persons and personal data can be reshaped through privacy enhancing technologies (PETs) in order to support data protection and compliance with the GDPR. It discusses how to bridge the gap between the law on paper and the law in practice using PETs. One type of PETs are edge-based personal information management systems (PIMS) that strive to give back control of the data to the user and minimize the need to use vulnerable people's personal data in the first place, which leads to less legal compliance problems. This will be discussed in-depth later in this PhD. The fourth chapter also includes theoretical discussions as exploring debates such as privacy-as-confidentiality versus privacy-as-control, property rights versus inalienable rights (how personal data should be viewed and defined) or edge computing versus cloud-based data processing are essential preconditions to being able to propose the most appropriate practical technological solutions.

As it was mentioned before, in this thesis, legal research does not only consist of doing documental analysis but also contains an empirical dimension. This PhD is an attempt at conducting interdisciplinary research. While Chapter 2 is mainly devoted to legal research, the empirical third chapter is an interdisciplinary endeavour while Chapter 4 focusses on theoretical legal debates, technical solutions and is heavily influenced by the computer science field.

Publications

As a final note to this introductory chapter, some parts of this thesis and the underlying work have been adapted into standalone articles that have been published or submitted to peer-reviewed journals, including:

- **Published article based on Chapter 2 of this thesis:** Stanislaw Piasecki and Jiahong Chen, 'Complying with the GDPR when vulnerable people use smart devices' (2022) 12(2) International Data Privacy Law 113 (https://academic.oup.com/idpl/article/12/2/113/6510568);

- **Published article based on one of this PhD programme's modules (inspired some sections of the thesis):** Stanislaw Piasecki, Lachlan Urquhart and Derek McAuley, 'Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards' (2021) 42 Computer Law & Security Review 105542 (https://www.sciencedirect.com/science/article/pii/S0267364921000157);

- **Published contribution to a book based on the work done within the 'Defence Against Dark Artefacts' project on privacy and security in the context of smart homes** (https://www.horizon.ac.uk/project/defence-against-dark-artefacts/): Derek McAuley, Jiahong Chen, Tom Lodge, Richard Mortier, Stanislaw Piasecki, Diana Andrea Popescu and Lachlan Urquhart, 'Human-centred home network security' in Crabtree et al. (eds), *Privacy by Design for the Internet of Things: Building Accountability and Security* (IET 2021);

- **Forthcoming article based on Chapter 4 of this PhD:** Stanislaw Piasecki, Jiahong Chen and Derek McAuley, ‘Putting the Right P in PETs: Normative Challenges for Protecting Vulnerable People’s Data through Privacy Enhancing Technologies’.

Chapter 2: The Legal Data Protection Landscape Related to the Use of Smart Devices by Vulnerable People in Their Smart Homes

This chapter identifies and discusses the most relevant data protection law provisions in the context of the use of smart devices by vulnerable people within their smart homes. Topics concerning the choice of a legal basis (Section 2.1) as well as relevant data protection principles (Section 2.2) are analysed, and the chapter is concluded (Section 2.3). These issues are crucial as processing of personal data is generally prohibited unless justified with one of the legal bases and compliant with all of the GDPR principles. The regulation explicitly states that 'processing shall be lawful only if and to the extent that at least one' legal basis applies (Art. 6), and that 'the principles of data protection should apply to any information concerning an identified or identifiable natural person' (Rec. 26). The ICO confirms that a valid lawful basis is mandatory to be able to process personal data.[57]

As a starting point, there is a need to ascertain the applicability of the GDPR. Art. 2(2) GDPR states that 'This Regulation does not apply to the processing of personal data' '(c) by a natural person in the course of a purely personal or household activity' (the household exemption). Before discussing relevant legal grounds for data processing through smart home products and other GDPR principles, it is relevant to mention the household exemption issue and why this thesis does not analyse it in this chapter. Firstly, Chapter 2 focusses on companies' compliance obligations and on legal bases applicable to data processing activities undertaken by private organisations. It does not evaluate legal grounds that could be used to process a vulnerable person's data within a smart home by natural persons (for example, by a vulnerable person's legal guardian) or to process other people's data by vulnerable individuals. It is worth noting in this context that there is currently no specific normative analytical framework that could be used in a smart home setting in order to determine the accountability of smart home dwellers for the processing of other people's data and when precisely the household exemption applies to them.[58]

[57] Information Commissioner's Office, 'Lawful Basis for Processing' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> accessed 1 July 2022.

[58] Jiahong Chen and others, 'Who is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' 10 International Data Privacy Law 279, 293.

Yet, the lack of a clear normative framework governing accountability in domestic uses of smart technologies may have implications for the more technologically-focussed Chapter 4 in the context of the larger issue of effective and GDPR compliant personal information management when vulnerable people use smart home devices, which can be either undermined or supported through technological architectures. Joint controllership and the household exemption 'determine who should and who should not be held responsible for data processing activities' and 'serve as a legal mechanism to assign responsibilities'.[59] While waiting for more legal clarity concerning the applicability of the household exemption (it is not the objective of this thesis to analyse this question in detail), certain technological architectures could reduce the consequences of the current uncertainty and promote organisations' compliance with other GDPR principles at the same time, which will be discussed in the fourth chapter of this thesis.

Section 2.1 Satisfying the Requirements of the Chosen Legal Basis by Adapting Measures to the Needs of Vulnerable People

The choice of the legal basis will differ depending on whether the data controller is processing ordinary or special category personal data (2.1.I). The consent mechanism needs to be adapted to the needs of vulnerable adults and children when the latter use smart devices (2.1.II). With regard to alternative legal bases, how does the performance of a contract (2.1.III), legitimate interests (2.1.IV) and vital interests (2.1.V) legal grounds apply in the same situation?

2.1.I Special Category and Ordinary Personal Data

Art. 6 of the GDPR sets out the possible legal bases an organisation can use to process personal data – namely consent, performance of a contract, a legal obligation of the controller, vital interests of the data subject, protection of the public interest and legitimate interests. The most relevant legal bases for organisations working on smart devices used by vulnerable people seem to be consent, performance of a contract, legitimate interests and vital interests, with an emphasis on the first three as the last one will apply only in rare circumstances. This section will discuss in which situation and how a specific legal basis should be implemented.

[59] Ibid 288.

The categories mentioned above apply to 'ordinary' personal data. However, there are also special categories of personal data that require stronger protection measures because of their sensitivity. Art. 9.1 of the GDPR lists those categories as data revealing 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership' as well as 'genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'. To be able to legally process special category personal data, an organisation must not only choose a lawful legal basis under Art. 6 of the GDPR but also satisfy a distinct condition under Art. 9.[60] Among the conditions for processing special category data, five are listed solely in Art. 9 of the GDPR while the other five are provided in Art. 9 but also further developed in the UK Data Protection Act 2018.[61]

According to Art. 9.2 of the GDPR, the bases for processing special category data are explicit consent; employment, social security and social protection (when permitted by Member State law); vital interests; not-for-profit bodies with a political, philosophical, religious or trade union mission; data already made public by the data subject; legal claims or judicial acts; reasons of substantial public interest; health or social care; public health; archiving, research and statistics.[62] If an organisation is basing its processing activities on grounds related to employment, social security and social protection, health or social care, public health or archiving, research and statistics, then it will also be required to satisfy the additional conditions set to process such data in UK's DPA.[63]

Several legal bases for ordinary personal data processing differ from those related to the processing of special category data. In the subsequent sections, this study will map the former to the latter in an attempt to highlight the differences and how organisations could approach them. For example, when special category data is processed, legitimate interests do not apply as a legal basis as such anymore. However, are there similar legal bases that could be used to process this category of data? This question is relevant to this thesis as there are many smart

[60] Information Commissioner's Office, 'Special Category Data' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/> accessed 1 July 2022.

[61] Data Protection Act 2018 (UK).

[62] Ibid; Information Commissioner's Office, 'Special Category Data' (n 60).

[63] Ibid.

devices currently being produced (especially in the health sector) that gather vulnerable people's special category data (such as the Activinsights band lifestyle analysis tool).[64]

2.1.II Taking Special Measures for Vulnerable People in the Context of Consent by Default

Certain conditions need to be satisfied for consent to be valid. How do they apply when vulnerable people use smart products? (2.1.II.A). There are parental consent requirements for organisations providing information society services (ISS) to children. Do smart devices offer ISS? (2.1.II.B) Data controllers are obliged to take into consideration the needs of vulnerable individuals when gathering their consent. What does this mean in practice? (2.1.II.C). Does consent allow organisations to profile vulnerable people through smart devices? (2.1.II.D) When special category data is processed, consent needs to be explicit. What does this signify? (2.1.II.E). Finally, the last question that this part of the thesis will answer is why the consent mechanism has been often criticised by academics and citizens (2.1.II.F).

2.1.II.A 'Ordinary' Consent Conditions

Consent is certainly one of the most commonly used legal bases in the IoT sector. Regardless of the opinion one may have concerning the effectiveness of this legal ground in ensuring that people understand what they are agreeing to and that they are conscious of the potential consequences of their choices, it is important to discuss conditions of lawful consent as it will surely remain widely used by all types of organisations. Fulfilling those conditions would at least decrease the many intentionally manipulative practices of consent management platforms on the web today (for example, it is often much more difficult to reject all tracking rather than accept it and those platforms widely use pre-ticked optional boxes).[65] If those manipulatives practices are used on websites, they are certainly also implemented in the IoT sector and in the billions of smart products used by vulnerable people within their homes.[66]

[64] Activinsights, 'Activinsights Band' (2021) <https://www.activinsights.com/products/activinsights-band/> accessed 1 July 2022.

[65] Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, April 2020).

[66] It should be noted that another important reason why consent may in some cases be the preferable compliance option is that it could also be required by other sector-specific legislation. For example, Article 5(3) of the ePrivacy Directive (sometimes colloquially known as the 'cookie law') may potentially apply to smart devices as they are likely to fall within the definition of a 'terminal equipment'. (Directive (EU) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the

According to Art. 8 of the Charter of Fundamental Rights of the European Union, personal data 'must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[67] The GDPR also affirms that processing of personal data should be lawful and fair (Rec. 39) and that it needs to be done on the basis of consent or another legitimate legal ground (Art. 6, Rec. 40). For consent to be valid, the GDPR requires it to be freely given, informed, specific and unambiguous (Art. 4, Rec. 32). This thesis underlines the importance of taking special data protection measures in relation to children (Rec. 38 GDPR) and vulnerable adults in this context.[68] It is the data controller's obligation to demonstrate that data subjects have provided valid consent (Rec. 42). There are guidelines on consent which can be found in the documents of the WP29. They explain in more detail what the conditions of freely given, informed, specific and unambiguous mean. Those

protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [2002] OJ L 201/37) Under that Article, 'the storing of information, or the gaining of access to information already stored' is allowed only in three situations: (a) consent is given; (b) it is solely for transmission of communications; or (c) it is strictly necessary for the provision of a service requested by the user. The ePrivacy Directive is currently undergoing a legislative overhaul and the Commission proposed to add a fourth permissive condition of web audience measuring in the new Article 8(1). (European Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2017/0003' (COD), Brussels, COM (2017) 10 final) It is however clear that the list of legitimising grounds under the ePrivacy framework is and will continue to be different from that under the GDPR, and further research is needed to establish how the overlap of the two legal frameworks will play out in the field of smart home technologies.

[67] Charter of Fundamental Rights of the European Union [2012] OJ C 326.

[68] Special data protection measures should also concern the extent to which a legal guardian is allowed to act on behalf of a vulnerable adult when the latter does not have the capacity to make informed data processing decisions. This question will be asked more frequently with the development of systems such as Lilli, which monitor the behaviour and electricity usage (through sensors and AI technology) of social care patients in their homes in order to identify potential health problems. (See Chris Baraniuk, 'Sensors and AI to monitor Dorset social care patients' (*BBC*, 2021) <https://www.bbc.com/news/technology-58317106> accessed 1 July 2022.) Similarly to the previous point, in the case of the virtual assistant 'Nadia' created by the Australian government to monitor health data and biometric data (through emotive-inducing AI and machine learning), how should we reconcile the legitimate interest of the State to improve access to government services by people with cognitive disabilities with their right to privacy and data protection? In this scenario, should legal guardians be able to give consent on behalf of a vulnerable individual? (See Nora Ni Loideain, Rachel Adams and Damian Clifford, 'Gender as Emotive AI and the Case of 'Nadia': Regulatory and Ethical Implications' SSRN Electronic Journal ssrn: 3858431 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3858431> accessed 1 July 2022.) Finally, Claire Bessant discusses the issue of 'sharenting' (sharing children's information online) and underlines that in the United Kingdom it is not certain when a parent's right to decide how their children's data is used gives way to the child's right to data protection. (See Claire Bessant, 'Sharenting: Balancing the Conflicting Rights of Parents and Children' (2018) 23(1) Communications Law 7.) These are all open questions that society needs to find a response to. A legal guardian should not have unlimited access to a vulnerable person's data as they might not always have good intentions or the capacity to make informed decisions on behalf of the person they are supposed to protect. Law provisions are unlikely to be a successful solution on their own and should be combined with technological developments in the field of data protection management to make them effective (such as personal information management systems and other privacy enhancing technologies). This topic has been further explored in Chapter 4 of this PhD.

conditions have also been analysed in legal literature. What kind of measures should be taken by organisations to obtain lawful consent from vulnerable people?

For consent to be freely given, the data subject must have genuine or free choice and must be able to refuse or withdraw consent without detriment (Rec. 42). In the context of smart devices, this would mean, for example, that consenting to physical tracking is not lawful in the case where the only other option is for the person to turn off the WIFI connection and, as a consequence, lose access to relevant services.[69] The GDPR adds that 'when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract' (Art. 7 (4) GDPR). There are different ways in which data subjects can be influenced and manipulated into agreeing to the processing of their personal data. However, not all external pressure invalidates consent.[70] Consent remains freely given when the exercised pressure is positive, while any sort of negative pressure exercised on the data subject makes the consent invalid.[71] A smart health device could underline the strong data protection measures that have been implemented into its design as a way to convince people to give their consent. If those claims were true and measures effective, this could be considered as an example of positive instead of negative or manipulative pressure. Consent will also not be freely given 'where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority' (Rec. 43). While this does not fall within the scope of this thesis, it could be relevant, for example, when public hospitals use smart products. They would need to reflect on the possibility of the existence of such an imbalance and how to make sure that consent is freely given.

When smart devices are being used by minors still under parental responsibility or adults with a legally authorised representative, this can further complicate the already complex implementation of consent requirements. In the case of the freely given consent condition, the situation can become more complex when children or vulnerable adults give their consent without the participation and awareness of their parents or legal guardian. Such situations can

[69] Claude Castelluccia and others, 'Enhancing Transparency and Consent in the IoT' (IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, April 2018).
[70] Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US footsteps?' (2017) 26(2) Information & Communications Technology Law 146.
[71] Ibid.

be problematic because their vulnerabilities can be exploited to influence and manipulate them. For example, children's increasing spending power online has been the subject of research papers as they are becoming more frequently targets of malicious commercial actors.[72] Similarly, adults with cognitive disabilities using a smart TV could be asked to consent and their consent exploited for financial reasons. Therefore, the freely given condition presents challenges when smart devices are being used by vulnerable individuals. Vulnerable people's choices and data management options depend on the functionalities and design of smart devices which should be adapted to their needs to ensure that consent is obtained from the legally authorised person. To increase chances for the latter to happen, it is imperative to satisfy all of the consent requirements.

Regarding the specificity condition, the WP29 clarified that the 'controller must apply; (i) Purpose specification as a safeguard against function creep, (ii) Granularity in consent requests, and (iii) Clear separation of information related to obtaining consent for data processing activities from information about other matters'.[73] The specification requirement of the information given to the data subject is an inherent element of informed consent. However, the fact that consent needs to be specific also concerns the degree of this specificity.[74] For consent to be valid, the legitimate data processing purposes must be explicitly specified (Rec. 39 GDPR). The GDPR adds that several processing activities conducted for the same purpose can be included in one consent request (Rec. 32). If, however, data is processed for multiple purposes, separate consent requests will be required for all of them (Rec. 32).

In the case of website cookies, controllers sometimes argue that data subjects have given consent for their data to be transferred to third parties by ticking a box. This does not seem to satisfy the specificity requirement as users will often still not know who exactly has access to their data and for what purpose. In the case of smart devices, the situation is even worst. If the always listening Amazon Echo smart speaker sends data to 'trusted third parties', intimate conversations could end up being analysed by real human beings, in remote places, for incomprehensible reasons to the data subject.[75] They cannot be said to have knowingly given

[72] Kathryn C. Montgomery, 'Youth and Surveillance in the Facebook Era: Policy Interventions and Social Implications' (2015) 39(9) Telecommunications Policy 771.

[73] Article 29 Working Party, 'Guidelines on Consent Under Regulation 2016/679' (WP 259, 2018).

[74] Macenaite and Kosta (n 70).

[75] Matt Day and Natalia Drozdiak, 'Thousands of Amazon Workers Listen to Alexa Users' Conversations' (*Time*, 11 April 2019) <https://time.com/5568815/amazon-workers-listen-to-alexa/> accessed 1 July 2022.

consent for this specific purpose. Even if Amazon responds that this is taking place to improve the operation of a smart device, it still does not seem specific enough. One cannot always justify data collection by the improvement of a product or service. More information should be given to the data subject, especially when smart devices are used by vulnerable adults or children as their situation and personal data can be particularly sensitive. Courts and regulators will need to interpret the provisions and decide what is the degree of specificity demanded from companies developing IoT products.

Concerning the unambiguity requirement, the GDPR explains that it means consent should 'be given by a clear affirmative act' (Rec. 32 GDPR). A crucial element in evaluating whether data subjects give lawful consent is to see if they clearly indicated their wishes.[76] The GDPR affirms that the data subject must indicate their choice to consent through a clear affirmative action or statement (Art. 4 (11) GDPR). It is not allowed to presume consent on the basis of inaction or silence of individuals.[77] As a consequence, consent cannot be obtained through pre-ticked boxes (Rec. 32). Rec. 32 adds that data subjects can indicate their wishes through a written statement (including electronically) or an oral expression of their choice. This could be done by ticking a box on a smartphone app through which a smart device is controlled, by choosing certain technical settings on an IoT device or another action which clearly shows the data subject's agreement to process data for a specific purpose. Any kind of personal data, such as a Media Access Control (MAC) address (a unique identifier of a specific device that wants to take part in a network), should not be gathered unless the consumer has opted-in for this data collection.[78] Concerning vulnerable people, the challenge here would be to ensure that children or vulnerable adults understand the consent requests, the choices they have and how to exercise them. For vulnerable individuals, the unambiguously given condition seems more closely linked to the informed consent requirement than in the case of ordinary citizens.

The unambiguously given consent requirement has not received unanimous support. For example, in the past, the UK chose not to include the expression of 'unambiguously given' consent in its Data Protection Act during the transposition of the Data Protection Directive.[79] Some authors argue that this condition does not add much value to the way consent is

[76] Macenaite and Kosta (n 70).
[77] Eoin Carolan, 'The Continuing Problems with Online Consent under the EU's Emerging Data Protection Principles' (2016) 32(3) Computer Law & Security Review 462.
[78] Castelluccia and others (n 69).
[79] Macenaite and Kosta (n 70).

considered.[80] Ambiguous consent would be equivalent to an unclear and unspecific expression of the decision of the data subject and would render consent invalid.[81] As a consequence, other consent conditions would already cover the unambiguously given requirement. However, this thesis considers the inclusion of this requirement into the definition of consent in the GDPR as a positive development. Such a change makes it even more clear to data controllers that pre-ticked boxes and similar ways to obtain consent will not be lawful. In the case of smart devices, any kind of data should be collected only after the data subject has opted-in for this to happen.

Finally, consent will only be informed if the data controller provides the data subject with information that is essential to make an informed choice (such as the controller's identity or the purpose for processing personal data).[82] Informed consent (Art. 4, Rec. 32) means that any communication to the data subject must be transparent (Art. 5). The transparency conditions are applicable 'irrespective of the legal basis for processing and throughout the life cycle of processing'.[83] They will be discussed in more detail in Section 2.I. of this chapter. Transparency and consent are closely related but they are distinct concepts within data protection law.[84]

2.1.II.B Information Society Services Directly Offered to Children

This study will now discuss the specificities of obtaining consent from children in the context of information society services (ISS) being used by the latter and whether smart devices qualify as ISS. Art. 8 of the GDPR introduces new requirements to ensure a higher level of protection of children's data when ISS are offered directly to them.[85] For the first time, European data protection laws demand parental consent from ISS providers before the latter are allowed to process personal data of children who are under 16 years old.[86] In the UK, this age limit has been lowered to 13 years old (this is the lowest age allowed by the GDPR).[87] Does Art. 8 apply to situations in which smart devices are being used by children?

[80] Eleni Kosta, *Consent in European Data Protection Law*, vol 3 (Brill/Martinus Nijhoff 2013) 235.
[81] Macenaite and Kosta (n 70).
[82] Article 29 Working Party, 'Guidelines on Consent Under Regulation 2016/679' (n 73).
[83] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (WP 260, 2017) (n 83).
[84] Information Commissioner's Office, 'Update Report into Adtech and Real Time Bidding' (20 June 2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf> accessed 1 July 2022 .
[85] Article 29 Working Party, 'Guidelines on Consent Under Regulation 2016/679' (n 73).
[86] Macenaite and Kosta (n 70).
[87] Data Protection Act 2018 (UK).

The term ‘information society service’ means ‘contracts and other services that are concluded or transmitted on-line’ and ‘normally provided for remuneration’.[88] ISS are not necessarily funded directly by the individual to whom they are offered (for example, online services paid for by advertisements).[89] It is clear that websites such as Facebook should be considered as ISS but what about IoT devices? Do services offered through smart devices fall within this scope? The ICO informs us in its ‘Age Appropriate Design: Code of Practice for Online Services’ that providers of ISS are organisations, which ‘provide online products or services (including apps, programs, websites, games or community environments, and connected toys or devices with or without a screen) that process personal data’.[90] Some IoT products are, therefore, included in this definition but does it mean that this can be said about every smart device? What does ‘normally provided for remuneration’ mean in the IoT context? There are smart devices which track user behaviour for advertising-related reasons (often without the knowledge of the data subject).[91] As a consequence, they would fall under the scope of the ISS definition. However, there are also many smart products that do not require advertising-related payments. For example, according to Amazon, Alexa does not normally gather your data for marketing purposes.[92] However, the service will be considered as ISS as long as there is '“economic activity” in a more general sense'[93]. If Alexa offers any types of services ‘typically provided on a commercial basis’ it will be defined as ISS[94]. Alexa does offer, for example, voice shopping services and, as a consequence, it should qualify as ISS. The ICO explains that this means the vast majority of online services are indeed ISS, except in specific circumstances such as in the case of counselling services offered directly to a child, certain services provided by public

[88] Article 29 Working Party, ‘Guidelines on Consent Under Regulation 2016/679’ (n 73); Ker-Optika, Case C-108/09, [2015] (ECLI:EU:C:2010:725); Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L 241.

[89] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market [2000] OJ L 178.

[90] Information Commissioner’s Office, ‘Age Appropriate Design: a Code of Practice for Online Services’ (n 26).

[91] EDPB, ‘Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects’ (16 October 2019) <https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_en> accessed 1 July 2022.

[92] Andrew Williams, ‘Smart Home Privacy: What Amazon, Google and Apple do with your Data’ (*The Ambient*, 2019) <https://www.the-ambient.com/features/how-amazon-google-apple-use-smart-speaker-data-338> accessed 1 July 2022.

[93] Information Commissioner’s Office, ‘Age Appropriate Design: a Code of Practice for Online Services’ 16 (n 26).

[94] Ibid.

authorities, general broadcast services, traditional voice telephony services and websites only giving information about a real-world service or business[95].

Concerning the 'direct offer' condition of ISS to children, the question is when is this requirement satisfied when smart products are being used by a child? The WP29 gives the example of a service provider that offers services uniquely to adults. According to the WP29, this type of service would not fall under the definition of being directly offered to children and Art. 8 would not apply.[96] However, what about services offered to all users? For example, in the case of smart devices, is Amazon's Alexa directly offering services to children? In its 'Age Appropriate Design' guide, the ICO has stated these guidelines 'are not restricted to services specifically directed at children' and that they apply to ISS 'likely to be accessed by children'.[97] As a consequence, while the GDPR is not specific enough to respond to this question, according to ICO's guidance Alexa would satisfy the direct offer requirement because children would likely access its services.

The GDPR does not give any practical advice on how to identify the person having the right to give consent on behalf of the child who does not have the capacity to consent[98]. The WP29 advises to adopt a proportionate approach to verify that consent has been given by an authorised individual and to obtain as little information as possible in the process (such as, only the contact details of a legal representative) in conformity with the data minimisation principle (Art. 5.1 (c) GDPR) and the 'reasonable efforts' requirement (Art. 8.2 GDPR).[99] The WP29 states that it is 'up to the controller to determine what measures are appropriate in a specific case' but that the controller should definitely avoid excessive data collection when trying to identify whether a person is old enough to provide consent or whether the adult providing consent on behalf of a child has the right to do so. If the data subject has gained the ability to consent, they must be able to confirm, modify or withdraw the previously given consent by the authorised holder of responsibility. The same guidelines would be applicable to vulnerable adults and their legally authorised representatives.

[95] Ibid.

[96] Article 29 Working Party, 'Guidelines on Consent Under Regulation 2016/679' (n 73).

[97] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).

[98] Article 29 Working Party, 'Guidelines on Consent Under Regulation 2016/679' (n 73).

[99] Ibid.

2.1.II.C Nature of the Special Measures Taken for Vulnerable People

One organisation which gives some advice in relation to the measures to be taken to obtain valid consent from vulnerable people (it also focusses specifically on children) is the ICO. The ICO states that privacy notices provided to children should be presented in a clear, plain and age-appropriate language; the manner of providing privacy-related information should be child friendly, for example, by using dashboards, cartoons, diagrams, graphics and videos, icons and symbols; explanations related to why children's data is processed, risks involved and safeguards implemented against the latter should be presented in a manner and language that children can understand.[100] This GDPR-influenced guidance is something new (Rec. 60 and Art. 12.7 GDPR). European Union data protection law had never before recognised the potentiality of illustrations to support individuals in comprehending data practices and, therefore, their decision-making.[101] According to the ICO, if an organisation decides to use consent as a legal basis for processing, it has to make sure that the child understands the privacy policy, otherwise consent will not be valid.[102]

Implementing the measures proposed by the ICO would not only benefit children but also adults with cognitive disabilities. This PhD argues that taking measures to ensure that privacy policies are understandable by all groups of people should be a standardised practice for organisations working on smart products. In terms of products developed for the general population and as Livingstone suggests, 'it may work better for data controllers to protect the rights (and limit the commercial exploitation) of all users than to try to identify children (and other vulnerable users) so as to treat them differently (not least because the very process of identifying children may undermine the principle of data minimisation which protects their privacy)'.[103] However, if a smart device is specifically developed for a particular group of vulnerable individuals, then special additional measures might need to be taken in conformity with GDPR requirements to adapt data protection measures to vulnerable people's needs. A data protection impact assessment might be a useful tool to evaluate if this is necessary and what actions should be taken. For example, people living with dementia can forget over time

[100] Information Commissioner's Office, 'Children' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/> accessed 1 July 2022.
[101] Arianna Rossi and Monica Palmirani, 'A Visualization Approach for Adaptive Consent in the European Data Protection Framework' (International Conference for E-Democracy and Open Government, Krems, May 2017).
[102] Information Commissioner's Office, 'Children' (n 100).
[103] Sonia Livingstone, 'Children: a Special Case for Privacy?' (2018) 46(2) Intermedia 18, 23.

that they have given consent to process their data. It is not clear how such special circumstances may affect the validity of the consent given by those persons.

2.1.II.D Consent Needed for Profiling of Vulnerable People

The ubiquity of personal data gathered through IoT devices, and the corresponding opportunities to detect correlations and to establish links, can lead to the analysis, determination and prediction of certain characteristics of a person's behaviour, personality, routines or interests. This profiling activity is defined in the GDPR as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour location or movements' (Art. 4.4). Rec. 38 of the GDPR explains that profiling is an area in which children need specific protection in relation to the use of their personal data. Rec. 71 adds that decisions based on automated processing of personal data 'should not concern a child'. It can be argued that such 'invisible processing' of the data of adults with cognitive disabilities will also violate the lawfulness, fairness and transparency principles (Art. 5.1).[104] They could have trouble comprehending what happens to their data and to what consequences profiling can lead.

Profiling and automated decision-making can help companies in saving resources and increasing efficiencies. However, those activities can also be damaging by preserving stereotypes, social exclusion and segregation as well as leading to imprecise predictions that can result in a denial of particular services and groundless discrimination.[105] For example, a smart device such as a voice assistant could potentially gather special category personal data by listening to a vulnerable adult's activities inside their smart home. It could then decide to restrict certain services or to target them with others based on their cognitive disability.

For those reasons, the ICO requires organisations to ensure that profiling is turned off by default on their smart products when they are being used by children (except if there is a compelling reason not to do so) and, because they are also inherently vulnerable, it should be

[104] Article 29 Working Party, 'Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679' (WP 251, 2018).

[105] Ibid.

turned off for adults with cognitive disabilities as well (if profiling is not crucial to the provision of the core service that has been requested).[106] This measure would be also beneficial to all other citizens. As it has been mentioned in the previous section, measures adopted for vulnerable individuals should become standardised practice for any smart product. This would make compliance and protection of personal data more effective for everyone.

The ICO underlines that turning profiling off by default does not signify that it is illegal (the ICO seems to follow WP29 guidelines on automated decision-making that take the same approach).[107] However, certain steps need to be taken to be able to process children's data based on profiling, in particular obtaining their consent to do so. Similarly, profiling and automated decision making would only be possible after receiving consent from adults with cognitive disabilities. Moreover, appropriate measures would need to be adopted to protect the child or vulnerable adult from any potentially negative consequences of profiling (such as being provided with content that is harmful to their wellbeing or health).[108]

ICO's guidance and interpretation does not seem appropriate as Rec. 71 explicitly and clearly prohibits profiling of children and taking automated decisions based on their personal data. Ultimately, courts will need to decide what interpretation is correct. Until that happens, this thesis argues that organisations should not profile children (or vulnerable adults) and their consent to profiling would be invalid. In certain unique cases there could be exceptions to the overall prohibition of profiling, for example, if automated decision-making could help in protecting other fundamental rights of a child considered essential for the latter in a specific situation. Until this is clarified, any unjustified profiling activities through smart devices should not be allowed.

2.1.II.E Special Category Data – Difference Between General and Explicit Consent

In terms of special category data, there is a corresponding legal basis to ordinary consent called explicit consent. While it is difficult to see major differences between general and explicit consent requirements, the EDPB tried to explain what additional measures a controller needs

[106] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).
[107] Article 29 Working Party, 'Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679' (n 104).
[108] Ibid.

to take to obtain explicit consent from the data subject.[109] Firstly, it stated that this could be done by confirming consent through a written statement. However, Rec. 32 already proposes written statements as a way of obtaining ordinary consent. The difference could lie in obtaining a signature of the data subject, which is also proposed by the EDPB, in addition to the written statement. One way of differentiating unambiguous and explicit consent could be the requirement of a signature. Secondly, the EDPB added that signed statements are not the only way to obtain explicit consent and the latter, in the online or digital context, could also be acquired by 'filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature'.[110] Here again, the first two propositions do not differ much from the written statement mentioned in Rec. 32 in relation to ordinary consent. However, scanning a signed document or providing an electronic signature could be the element tipping the balance in favour of the existence of explicit consent in the digital context. Thirdly, the EDPB mentioned oral statements as another possibility while adding that in this case, it could be difficult for the controller to prove that all conditions of explicit consent have been met. Oral expression of the data subject's choice is also mentioned in relation to ordinary consent conditions. It is difficult to see the difference between explicit and unambiguous consent in this scenario. Finally, the guidelines propose a two-stage verification of consent as a way to prove that explicit consent has been obtained. For example, the controller could ask the data subject to send an email containing the statement 'I agree' for the data to be processed and to also click a verification link to confirm their choice. To conclude, in the context of smart devices, a two-step verification process or obtaining a digital signature from the data subject (in addition to all of the previously mentioned ordinary consent conditions) seems necessary if the organisation in question decides to process special category data. In the current state of the IoT sector, many devices used by vulnerable individuals (voice assistants, smart TVs, smart health devices etc.) do (or might) collect special category data and those additional explicit consent requirements would most probably apply in many situations. For example, Amazon was recently sued for allegedly recording children without their or their legal guardians' consent. The complaint stated that 'at no point does Amazon warn unregistered users it is creating persistent voice recordings of their Alexa

[109] EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (2020) 21 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 1 July 2022.

[110] Ibid.

interactions, let alone obtain their consent to do so'.[111] At the time of these events, Alexa's privacy notice only informed that previous voice requests are analysed to improve its functioning but did not explicitly state that humans listen to them. Such voice recordings can contain special category data of vulnerable individuals and if the complaint had been raised in an EU context, Amazon's activities would be most probably considered as violating GDPR's provisions. In this case, Amazon should have ensured a two-step consent verification process is in place, adapted to the needs of children using its devices. Strong enforcement mechanisms are required to ensure the consent requirements are met.

2.1.II.F An Uncertain Effectiveness of the Consent Mechanism

Consent is not universally accepted as a useful mechanism and it has been criticised by various authors, in particular in the context of vulnerable people's data collection. Some researchers contend that consent gives an illusion of control[112] and that it is often given in the context of an imbalance of powers so not accorded freely.[113] Several articles underline the nature of networked environments that establish power imbalances and reduce people's influence and control over their own personal data.[114] Vulnerable people such as children cannot fully control their personal data online because their decisions and data management options depend on the functionalities and design of communication spaces.[115] This is true for smart devices as well. Communication spaces are designed by organisations, so usually, unless the organisation is a charity or similar actor (or there is a financial incentive), it will design it in a way to promote its own business interests. Smart devices asking for consent often use hardly understandable privacy policies and users do not actually familiarise themselves with them. Privacy policies for children are especially confusing, difficult to comprehend, often long and complex.[116] Organisations developing smart devices could be hopefully forced to change their behaviour if enforcement, and the resulting effective implementation of GDPR, gains momentum. For this

[111] Leo Kelion, 'Amazon Sued over Alexa Child Recordings in US' (*BBC*, 13 June 2019) <https://www.bbc.com/news/technology-48623914> accessed 1 July 2022.

[112] Laura Brandimarte, Alessandro Acquisti and George Loewenstein, 'Misplaced Confidences' (2013) 4(3) Social Psychological and Personality Science 340.

[113] Macenaite and Kosta (n 70).

[114] Mireille Hildebrandt, 'Profiling and the Rule of Law' (2008) 1(1) Identity in the Information Society 55; Macenaite and Kosta (n 70).

[115] Alice E. Marwick and Danah Boyd, 'Networked Privacy: How Teenagers Negotiate Context in Social Media' (2014) 16(7) New Media & Society 1051; Macenaite and Kosta (n 70).

[116] Anca Micheti, Jacquelyn Burkell and Valerie Steeves, 'Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand' (2010) 30(2) Bulletin of Science, Technology & Society 130.

to happen, more funding should be dedicated to currently underfunded data protection authorities.[117] An interesting idea is for designers to support regulators (and not just data subjects or platforms) by designing automated tools allowing for quick discovery of GDPR violations and enforcement.[118] This idea was presented in the context of dark patterns associated with most current consent management platforms. Such automated tools could potentially also be designed for IoT products.

Even if privacy notices are written in clear terms, it is widely known that people rarely read them.[119] Some have even suggested that, ironically, the most important practical impact creating privacy notices is not in providing information to consumers but 'in informing the companies that are collecting and using the data and in improving the companies' management of privacy'.[120] This is why consent should be combined with other mechanisms providing relevant information to users after they have consented such as contextual pop-ups explaining how data is processed by an IoT product and allowing the data subject to easily change the settings (this will be discussed in Section 2 of this chapter). However, this thesis considers data protection by design and by default as well as data minimisation as the most crucial mechanisms that can limit the number and the negative effects of incomprehensible privacy policies communicated to vulnerable people (they will also be discussed in Section 2).

2.1.III Evaluating the Perspective of an Average Data Subject before Processing Vulnerable People's Data Based on a Contract

When can an organisation use the performance of a contract legal basis (2.1.III.A) and how is this applicable in the context of a smart device such as a smart TV? (2.1.III.B) Is there an equivalent legal basis when an organisation developing or deploying smart products processes vulnerable people's special category personal data? (2.1.III.C)

2.1.III.A The Applicability of the Performance of a Contract Legal Basis

[117] Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8(2) International Data Privacy Law 105, 105.
[118] Nouwens and others (n 65).
[119] Claudia Diaz, Omer Tene and Seda Gurses, 'Hero or Villain: the Data Controller in Privacy Law and Technologies' (2013) 74(6) Ohio State Law Journal 923.
[120] Daniel J. Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126(7) Harvard Law Rev 1880, 1900.

Firstly, while Art. 6.1 (b) concerns contracts, this thesis does not analyse the validity of contracts related to smart devices in a comprehensive manner as this is outside of its scope. However, it is important to mention that contracts and their terms need to abide by the conditions set out in the law of contracts, and consumer protection legislation for consumer contracts, to ensure that data processing based on contractual terms conforms to the principles of lawfulness and fairness. A pertinent example is the case of children. Apart from complying with specific measures dedicated to children in the GDPR, the data controller has to make sure that it acts in compliance with applicable national legislation concerning the capacity of children to enter into contractual relationships.[121] The ICO confirms that if the contract is with someone under 18 years old, organisations need to reflect whether this person has the required competence to enter into a contract and whether they understand what they are agreeing to.[122] If the data controller is unsure about a child's competence, it should consider whether an alternative legal basis (for example, legitimate interests) would be more appropriate in terms of proving that a child's interests and rights are well protected and safeguarded when their data is being processed. This reasoning will also apply to adults with cognitive disabilities. If contract law does recognise a person's competence to enter into a contract in a particular situation, does that automatically mean the data processing is lawful? The response is in the negative as the data controller needs to satisfy GDPR requirements to be able to use the performance of a contract legal basis to process vulnerable people's personal data.

The performance of a contract legal basis is lawful when processing personal data is 'necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract' (Art. 6.1 (b) GDPR). Rec. 44 confirms that 'processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract'. The data subject must reasonably expect the use of this legal basis by the data controller. As a consequence, consent differs from the performance of a contract legal basis. They have different requirements. According to the EDPB, it is important to make a distinction between consent and performance of a contract 'as these concepts are not

[121] EDPB, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (n 91).

[122] Information Commissioner's Office, 'Contract' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/> accessed 1 July 2022.

the same and have different implications for data subjects' rights and expectations'.[123] As it has been explained in the section on consent, the latter must be specific, freely given, informed and unambiguous whereas processing on the basis of a contract must satisfy the necessity condition. The more stringent consent requirements would, in principle, make the data subject more aware of how their data is processed than in the case of the performance of a contract legal basis.

The concept of necessity is not just an evaluation of what is allowed by or included in the terms of a contract. This concept has its own independent meaning and must reflect data protection law's goals.[124] The ICO explains that 'necessary' does not signify that the processing has to be the unique and crucial way to perform a contract but it needs to be 'more than just useful, and more than just part of your standard terms'.[125] The necessity condition has to be interpreted strictly.[126] It does not cover situations where processing is not genuinely necessary to perform a contract.[127] It has to be a 'proportionate and targeted step', that is an essential part of the action or service needed to be accomplished according to the contract.[128] If the action or service can be reasonably performed by processing a smaller amount of data or in a less invasive manner, this legal basis will not be valid. If processing is not essential for the performance of a contract with a particular person but necessary for the operation of a specific business model or incorporated into the terms for other business reasons, not related to performing the contractual obligation, the data controller also needs to choose another lawful legal basis.

The data controller has to be able to explain the necessity of personal data processing 'by reference to the fundamental and mutually understood contractual purpose'.[129] The controller should carefully evaluate the 'perspective of an average data subject' to ensure that the purpose of data processing is mutually genuinely understood.[130] The ICO advises organisations to document why they have decided to process data on the performance of a contract legal basis

[123] EDPB, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (n 91).

[124] Ibid.

[125] Information Commissioner's Office, 'Contract' (n 122).

[126] EDPB, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (n 91).

[127] Kristina Irion and Natali Helberger, 'Smart TV and the Online Media Sector: User Privacy in View of Changing Market Realities' (2017) 41(3) Telecommunications Policy 170; EDPB, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (n 91).

[128] Information Commissioner's Office, 'Contract' (n 122).

[129] EDPB, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (n 91).

[130] Ibid.

and to ensure that this choice can be convincingly justified by the company.[131] This is especially important in light of certain opaque IoT contracts. For example, contracts related to the Google Nest Smart Home system have been considered as 'difficult to understand' in terms of 'the protection actually granted to a user's personal data'.[132] They are difficult to comprehend even for legal experts. This means that they do not satisfy the performance of a contract legal basis requirement of explaining the necessity of personal data processing and why the latter should be understood by data subjects.

In summary, organisations will only be able to process personal data of children and vulnerable adults if this is necessary to perform the contract and if they expect and understand the purpose of this processing. If the necessity condition is not satisfied or if they want to process data outside of the contract's scope, they will need to rely on a different legal basis. A smart TV example will be now analysed. Smart TVs are often used by vulnerable people and the next section will consider whether performance of a contract is an appropriate legal basis for data processing in this context.

2.1.III.B Performance of a Contract and Smart TVs

When a vulnerable person buys a smart TV, can the service providers rely on the sales contract to collect personal data without asking for consent? Before answering this question, it is important to establish what kind of data a smart TV is able to collect. Firstly, some of these devices have voice recognition capabilities. A smart TV can record sounds nearby and recognise speech patterns that can be then registered and used as commands.[133] Such a device could pick up information allowing to directly or indirectly identify natural persons as it is often placed in a central location of a household and, therefore, falls within the scope of the GDPR. This information could or not include special category personal data. Art. 4.2 of the GDPR states that processing means, among others, collecting, recording and transmitting information. As a consequence, a smart TV recording sounds in its surroundings can be considered as a device processing personal data. Some smart TVs can also recognise a person's

[131] Information Commissioner's Office, 'Contract' (n 122).

[132] Guido Noto La Diega and Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest' (2016) 7(2) European Journal of Law and Technology 1, 9.

[133] Britt Van Breda and others, 'Smart TV and Data Protection' (*European Audiovisual Observatory*, 2016) 56-60 <https://rm.coe.int/iris-special-2015-smart-tv-and-data-protection/1680945617> accessed 1 July 2022.

face. Images are almost certainly personal data that can be considered special category data if, for example, a person's ethnicity can be deduced from the image.[134] Both in the case of sound recordings and facial recognition, there is a risk that personal data of guests or other people not ordinarily present in the household could be collected and processed. Smart TVs could also collect personal data through the creation of a user account by requiring the user to provide, for example, their name.

As we have seen above, the necessity condition needs to be interpreted strictly and processing will only be lawful if it is essential to the performance of a contract. In an investigation concerning visual and audio personal data processing through Philips smart TVs by TP Vision, the Dutch data protection authority declared that 'a justification for the processing must be present in relation to the specific, individual data subject involved'.[135] Buying a smart TV is essentially a sales contract that has not much to do with audio or visual data. The performance of a contract legal basis is not the right legal basis to process personal data in this context. If a person is vulnerable, this would make the use of this legal basis even less appropriate. It is not possible to expect an ordinary person and even less a child or an adult with cognitive disabilities to know that by turning on a TV and clicking 'I agree' at the end of long terms and conditions, they sign a contract for their vocal and visual personal data to be processed. The data controller needs to evaluate the perspective of the user to ensure that they genuinely understand the purpose of data processing. This kind of evaluation would not have a positive outcome in this context.

2.1.III.C Special Category Data – Contracts, Medical Diagnosis and Provision of Health Care

Concerning the processing of special categories of personal data, the WP29 has underlined that the performance of a contract legal basis cannot be used as an exception to the overall interdiction to process special category personal data.[136] As a consequence, data controllers need to look for possible relevant exceptions in Art. 9.2 (b) to (j) GDPR. If none of those exceptions can be used as a legal basis, explicit consent will be the only option to process data lawfully.[137]

[134] Ibid.
[135] Ibid 60.
[136] Article 29 Working Party, 'Guidelines on Consent Under Regulation 2016/679' (n 73).
[137] Ibid.

In the case of adults with cognitive disabilities and children, there are smart products collecting health data that could be necessary, for example, for the purposes of a medical diagnosis or the provision of health care. In this situation, Art. 9.2 (h) GDPR could apply and provide for a special category legal basis that is related to and could be used in combination with performance of a contract. This article states that processing of special category personal data is allowed when it is 'necessary for the purposes of preventive or occupational medicine', for 'medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional'. A contract with a health professional could therefore allow to lawfully process special category data of a vulnerable person gathered through a smart product. Art. 9.2 (h) is especially relevant to vulnerable individuals as it concerns situations, in which health is the central reason for data processing.

Apart from health-related situations described above, special category data gathered by smart devices would require explicit consent. In the case of the smart TV example, if this device was developed to collect video or audio data, the data controller would first need to seek explicit consent from its customers.

2.1.IV Balancing the Legitimate Interests of a Data Controller Against Those of Vulnerable People

Is legitimate interest an appropriate legal basis to process vulnerable people's personal data when they use smart products? (2.1.IV.A) Is there a corresponding special category legal basis that could be used in this context? (2.1.IV.B)

2.1.IV.A The Applicability of the Legitimate Interests Legal Basis

Legitimate interests have become frequently used as a legal basis to process personal data, especially in the commercial and new technologies field (for example, by Google).[138] For example, in relation to its Nest smart home devices, Google states that it may process individuals' information 'to pursue legitimate interests such as providing, maintaining and

[138] Federico Ferretti, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?' (2014) 51(3) Common Mkt Law Rev 843.

improving our services to meet the needs of our users'.[139] According to Art. 6.1 (f) of the GDPR, processing personal data is lawful when it is 'necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.' The use of the term 'in particular' suggests that the balancing exercise concerning processing of children's personal data will be stricter.[140] However, is this true in practice? How much stricter and what does this specifically entail?

The ICO advises organisations to take 'extra care' to protect children's rights and freedoms from risks they might not fully understand and from effects they may not predict if they desire to use legitimate interests as the legal basis for processing their personal data.[141] This requires an in-depth analysis of the objective and nature of the processing, and the possible risks for children. Because of the phrasing of Art. 6.1 (f), some authors consider rather unlikely that the legitimate interests of the data controller will prevail over those of the child.[142] A 'more compelling' interest would be required to legitimise any possible effect on children (the ICO recommends performing a data protection impact assessment).[143]

If a compelling interest can be identified, risks to children's rights would need to be mitigated as much as possible.[144] Taking relevant measures to protect them is necessary. For example, age appropriate safeguards would need to be implemented. In the Age Appropriate Design report, the ICO added that privacy settings are not only relevant in the context of consent but can also

[139] Google, 'Technologies' (2021) <https://policies.google.com/technologies/partner-sites?hl=en-US> accessed 1 July 2022.

[140] Milkaite Ingrida and others, 'The General Data Protection Regulation and Children's Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society. Roundtable Report' (*Ghent University*, 2017) 12 <https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf > accessed 1 July 2022.

[141] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26); Information Commissioner's Office, 'Legitimate Interests' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/> accessed 1 July 2022.

[142] Van Breda and others (n 133).

[143] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).

[144] Centre for Information Policy Leadership, 'GDPR Implementation in Respect of Children's Data and Consent' (5 March 2018) 6 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf> accessed 1 July 2022.

be implemented when a different legal basis is used (such as legitimate interests) to give children a voice over how their personal data is processed (this would also constitute an additional safeguard).[145] Adults with cognitive disabilities should also benefit from appropriate protection measures if the legitimate interests legal basis is used by a data controller. The WP29 confirms this by underlining that during the legitimate interests balancing test, the status of the data subject is important and that it is relevant to consider whether the data subject is a vulnerable person requiring special protection 'such as, for example, the mentally ill, a student, a patient, or whether there is otherwise an imbalance in the relationship'.[146] Just like children, adults with cognitive disabilities are also inherently vulnerable and, therefore, the balancing exercise would also need to be stricter and safeguards more robust. The nature of those should be further discussed as there are not many guidelines on this point but making settings customisable is one idea. If such safeguards are implemented by default by data controllers when they have a compelling reason to use legitimate interests, this would facilitate GDPR compliance and increase data protection.

Legitimate interests can be an appropriate legal basis when an organisation plans to use someone's personal data in ways that this person would reasonably expect and that have only a minimal impact on privacy, or in the case where there is a convincing reason for the processing.[147] Rec. 47 of the GDPR explains that there is a 'relevant and appropriate' relationship between the controller and data subject, for example, when the data subject is the controller's client or works for the controller. In any case, a careful assessment needs to be conducted to evaluate whether the data subject will reasonably expect at a certain time and in a specific context that their personal data will be gathered by the data controller.[148]

An organisation, which uses legitimate interests, should be aware that it needs to be able to convincingly explain why it has decided to use this legal ground in case a data protection authority demands this information. It would need to be able to prove that its interests are not 'overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data', in particular when the data subject is a vulnerable person

[145] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).

[146] Article 29 Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC ' (WP 217, 2014).

[147] Information Commissioner's Office, 'Legitimate Interests' (n 141).

[148] GDPR, recital 47.

(Art. 6.1 (f) GDPR). If it struggles with the balancing exercise or with the adoption of relevant protection measures, a different legal basis will be more appropriate.

One of the objectives of a smart TV seller is to provide a platform for advertisements and the associated analysis of viewer behaviour.[149] However, this kind of data processing is not essential to the provision of the main service. The ICO calls this 'non-core' processing.[150] In this scenario, it is unlikely that the vulnerable adult or child would reasonably expect that their data will be processed for advertising reasons. Moreover, no compelling interest seems to exist here that would override the need to protect fundamental rights and freedoms of vulnerable individuals. In this context, the service provider should probably rely on consent instead of legitimate interests and give the data subjects the choice to switch on different additional elements of the service whenever this is technically possible (instead of turning them on by default).

According to one opinion, the use of the legitimate interests legal basis by a data controller will often necessitate deeper reasoning, strategizing and attention for lawful implementation in comparison to only asking for consent.[151] Considering that the legitimate interests legal basis entails a balancing of interests and risk assessment, paired with the necessity to adopt suitable mitigating measures and accountability from data controllers, it could be a solid framework for analysing risk on an individual basis and permitting for particular risks to be addressed in specific situations (in keeping with this logic, it would help in adapting measures to the interests of children and adults with cognitive disabilities).[152] As such, and if implemented properly, legitimate interests could positively support the compliance with, and thus the effective functioning of, other parts of the data protection legal framework, such as DPIAs, which will be further discussed in Chapter 2, Section 2.2.V.

However, it should equally be noted that the above-mentioned opinion assumes that organisations actually take time and effort to do the in-depth balancing tests. In the past, there have been reports that legitimate interests are seldom reviewed in practice.[153] Other authors

[149] Van Breda and others (n 133).
[150] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).
[151] Centre for Information Policy Leadership, 'GDPR Implementation in Respect of Children's Data and Consent' (n 144).
[152] Ibid.
[153] Bits of Freedom, 'A Loophole in Data Processing' (11 December 2012) <https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf> accessed 1 July 2022.

point out that the balancing exercise is difficult and that it should not be performed only by data controllers.[154] The test necessitates a significant level of legal expertise and puts data controllers in a situation of 'clear conflict of interest'.[155] There is an intrinsic imbalance of power between the controller who determines whether a legitimate interest exists and the data subject who needs to accept the decision of the controller. Companies should be prevented from processing vulnerable people's data based on unbalanced 'legitimate interests', for example, if they establish profiles of children, which is in general prohibited. However, enforcement is not easy in the field of data protection, as data subjects do not often go to court without visible damage and an opportunity for redress (that is for compensation for harm or injuries sustained). They have limited incentive to do so and limited understanding of how their data is being processed.[156] Effective enforcement of the law is therefore key to ensuring the legitimate interests ground plays its role in safeguarding personal data rather than being abused to mis-legitimise unfair data uses.

In conclusion, there are different opinions as to the utility and effectiveness of the legitimate interests legal basis in protecting data subjects' rights. It is to be expected that if organisations do not fear enforcement action, not all of them will be performing effective balancing exercises. Considering the increasing ubiquity of smart devices, children and adults with cognitive disabilities will be using them more frequently. While smaller organisations might struggle with such a balancing exercise because of the lack of legal expertise or funds to hire a lawyer (maybe more public funds should be dedicated to free data protection advice for those organisations), big companies do not have any excuses not to perform a balancing test and should be held accountable if they do not, especially when their products are used by vulnerable people who require additional protection measures.

2.1.IV.B Special Category Data – Inapplicability of the Legitimate Interests Legal Basis in the Context of Smart Devices

Legitimate interest is not listed as an exemption to the general prohibition on processing special category data under Art. 9 GDPR as such, but some specific interests are explicitly recognised in that provision. A data controller who wants to use the legitimate interests legal basis and

[154] Ferretti (n 138).
[155] Ibid.
[156] Ibid.

process special category personal data could do so under, for example, Art. 9.2 (b) GDPR, which allows this category of data to be processed if it 'is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject'. However, this thesis looks at the smart home setting. Consequently, Art. 9.2 (b) will not apply and the data controller will need to look for another lawful legal basis. Other similar exemptions under Art. 9(2) are also unlikely to apply to this context, making explicit consent the most plausible choice for justifying the use of special category data.

2.1.V The Rarely Used Vital Interests Legal Basis

Art. 6.1 (d) of the GDPR states that an organisation can process personal data when this is 'necessary in order to protect the vital interests of the data subject or of another natural person'. Rec. 46 adds that 'processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis'.

Rec. 46 shows unambiguously that vital interests will only cover interests that are crucial for a person's life. As a consequence, the scope of this legal basis is very limited. It will only apply to 'matters of life and death'.[157] The ICO underlines that if an organisation processes someone's personal data to protect another person's vital interests, it should try to find a different legal basis, unless this is not possible. In this particular situation, an example of a legal basis that could be considered is legitimate interests as this lawful basis permits to balance the rights and interests of the data subject with the vital interests of the person the data controller is trying to help.[158]

In the majority of cases, a situation in which vital interests will need to be protected will arise in relation to health data. Health data is one of the special categories of data and, therefore, requires to satisfy a condition for processing under Art. 9 of the GDPR in addition to the

[157] Information Commissioner's Office, 'Vital Interests' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/> accessed 1 July 2022.
[158] Ibid.

condition from Art. 6.[159] One of the special conditions for processing health data is to protect a person's vital interests (Art. 9.2 (c)). However, the data subject must be incapable of giving consent for this condition to apply. For this reason, explicit consent will be the more relevant legal basis in many situations.[160]

Are there situations in which the vital interests legal basis could apply in the context of the use of smart devices by vulnerable adults with cognitive disabilities or children? Recently, researchers from the Netherlands have created a high-tech smart bracelet, the 'Nightwatch', capable of detecting 85 percent of night-time epileptic seizures and 96 percent of the most severe ones.[161] This is a considerably higher percentage than what other comparable devices can accomplish today.[162] The researchers tested the device with 28 intellectually disabled participants. This kind of wearable smart technology can potentially save lives by preventing seizure-related deaths. Smart watches help their users to monitor their own health, for example, by recording heart rates. The Nightwatch has the ability to go further and inform caregivers about severe seizures happening during the night. This could be a vital product for those affected by epilepsy as sudden unexpected death in epilepsy is the major cause of death for those living with the condition and for adults with a mental disability the risk of dying is even higher.[163] If the vulnerable data subject is not capable of giving consent but wears the Nightwatch smart bracelet, processing his personal data to find him on time and help him during a serious epileptic seizure must satisfy the necessity to protect vital interests condition.

It can be concluded from the above that organisations will use the notion of vital interests of the data subject to justify the processing of vulnerable people's personal data rarely, that is only when the latter are not capable to consent and when it's a matter of life and death. These situations could arise when personal data collected by smart devices has the potential to save lives.

[159] Ibid.

[160] Ibid.

[161] Johan Arends and others, 'Multimodal Nocturnal Seizure Detection in a Residential Care Setting: A Long-Term Prospective Trial' (2018) 91(21) Neurology e2010.

[162] The Guardian, 'High-Tech Epilepsy Warning Device Could Save Lives' (11 January 2019) <https://guardian.ng/features/health/high-tech-epilepsy-warning-device-could-save-lives-2/> accessed 1 July 2022.

[163] Eindhoven University of Technology, 'New Epilepsy Warning Device Could Save Thousands of Lives' (26 October 2018) <https://www.tue.nl/en/news/news-overview/24-10-2018-new-epilepsy-warning-device-could-save-thousands-of-lives/#top> accessed 1 July 2022.

Section 2.2 The Implementation of GDPR Principles when Vulnerable People use Smart Devices

Firstly, it should be noted that this thesis does not analyse all data protection principles in detail. The principle of purpose limitation demands to process personal data only for the original (or compatible) purpose of its collection.[164] The purpose of data processing has been briefly mentioned when discussing the specificity condition of lawful consent in Chapter 2, Section 1.II. While purpose limitation is certainly important both for ordinary and vulnerable citizens, this PhD does not analyse it in detail in this section as other principles seem more relevant in the specific context of smart devices used by vulnerable individuals. Similarly, the principles of accuracy and storage limitation will also not be analysed in-depth in this thesis. However, even if a separate section has not been dedicated do them, they will be mentioned when relevant in other parts of this study.

The overarching accountability principle is discussed in various places. This principle has an internal and external dimension. Firstly, it requires any data controller to implement systems, policies and procedures in order to prove to itself that its processing activities are compliant with the GDPR.[165] Requirements of this internal dimension of accountability can be met through means such as data protection impact assessments (DPIAs). The latter are particularly important for vulnerable data subjects using IoT products and they will be discussed in detail in this section. However, the accountability principle also has an external focus, which does not reduce itself to DPIAs.[166] An organisation that wants to demonstrate compliance with the accountability requirement should be compliant with the regulation in general and, therefore, be able to show that it meets conditions related to data minimisation, fairness, transparency, and other GDPR provisions. Those principles will be analysed in this section, in the special context of smart devices used by vulnerable individuals.

The lawfulness principle requires the processing to take place on the basis of a legitimate ground and the various legal bases have already been analysed in the first section of this

[164] Maximilian Von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation* (1 edn, Nomos Verlagsgesellschaft mbH 2018).

[165] Andy Crabtree and others, 'Building Accountability into the Internet of Things: the IoT Databox Model' (2018) 4(1) Journal of Reliable Intelligent Environments 39.

[166] Ibid.

chapter. The other most relevant principles for this thesis are the principles of transparency (2.2.I), fairness (2.2.II), data minimisation (2.2.III), data protection by design and default (2.2.IV) as well as integrity and confidentiality (2.2.VI). Finally, as it has been mentioned above, DPIAs will also be examined in this section (2.2.V).

2.2.I The Principle of Transparency and the Right to be Informed

In this part, a more in-depth look is taken at the right to transparent information and communication in the context of vulnerable individuals and smart products. Firstly, a definition of transparency is given (2.2.I.A). Secondly, the transparent, concise, intelligible and easily accessible information conditions (2.2.I.B) as well as the plain and clear language requirements (2.2.I.C) are discussed. Subsequently, the thesis reflects on how other GDPR mechanisms can foster transparency (2.2.I.D). Finally, the chapter is concluded by evaluating the relationship between transparency, vulnerability and IoT devices (2.2.I.E).

2.2.I.A Defining Transparency

This thesis discusses the principle of transparency separately from consent, as informed consent is only one area in which information needs to be provided in a transparent manner. Where processing in question is not based on consent, provision of information is still required under the GDPR. The right to transparent information and communication covers a wider range of situations in the GDPR. It is a crucial right, especially relevant to vulnerable people. Transparency is needed to avoid a gradual walk into a 'black box society', in which our data is recorded on devices and the workings of this system remain mysterious to users.[167] If data is collected without transparent information and communication about that process, vulnerable individuals will not be able to effectively exercise their rights such as the right of access (Art. 15 GDPR), right to rectification (Art. 16 GDPR), right to erasure (Art. 17 GDPR), right to restriction of processing (Art. 18 GDPR), right to data portability (Art. 20) or right to object (Art. 21).[168]

[167] Frank Pasquale, *The Black Box Society: the Secret Algorithms that Control Money and Information* (Harvard University Press 2016).

[168] Advocate General Cruz Villalón has confirmed this at paragraph 74 of his opinion in relation to the Bara case by stating that 'the requirement to inform the data subjects about the processing of their personal data, which guarantees transparency of all processing, is all the more important since it affects the exercise by the data subjects of their right of access to the data being processed, referred to in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive' (Pedro Cruz Villalón,

The principle of transparency is enshrined in Art. 5.1 (a) of the GDPR which states that personal data has to be 'processed lawfully, fairly and in a transparent manner in relation to the data subject'. Transparency is, therefore, an essential component of lawful processing. It is also 'an expression of the principle of fairness'.[169] If organisations do not adopt special measures to help vulnerable people understand how their information is processed and how they can exercise their GDPR rights, the latter would be at a disadvantage and organisations would be at risk of receiving fines. Art. 5.2 of the GDPR requires data controllers to be able to prove transparency under the new GDPR principle of accountability. This section discusses in more detail how the GDPR and guidelines present the right to transparent information and communication, specifically in the context of vulnerable individuals.

The ICO gives some advice concerning the principle of transparency on its website and in its guide to the GDPR but the most comprehensive guidelines on transparency are provided in the document written by the WP29.[170] According to the latter, transparency covers three important areas of the GDPR: '1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights'.[171] The main GDPR articles concerning transparency in relation to the rights of data subjects are Art. 12 (general requirements), Art. 13 and 14 (providing information to data subjects), Art. 15 – 22 (communicating with data subjects in relation to the exercise of their rights) and Art. 34 (communicating with data subjects concerning data breaches).

Transparency is not defined in the GDPR. However, GDPR recitals and articles are informative as to the meaning and effect of the principle of transparency in the context of data processing.

'Opinion of Advocate General Cruz Villalón Pedro delivered on 9 July 2015, Case C-201/14, Smaranda Bara and Others,' (9 July 2015) <https://curia.europa.eu/juris/document/document.jsf?docid=165642&doclang=en> accessed 1 July 2022); Bart Custers and others, 'A Comparison of Data Protection Legislation and Policies Across the EU' (2018) 34(2) Computer Law & Security Review 234.

[169] Charter of Fundamental Rights of the European Union (n 67); Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

[170] Information Commissioner's Office, 'Right to be Informed' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/> accessed 1 July 2022; Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83); Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)' (2018) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> accessed 1 July 2022.

[171] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

Rec. 39 underlines, among others, that 'it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed'. According to Art. 12, information must be concise, transparent, easily accessible and intelligible (Art. 12.1); the language must be clear and plain, especially when information is provided to children (Art. 12.1); information should be provided in writing or by other means when this is appropriate (including electronic means) (Art. 12.1); it should be provided orally when data subjects request to provide information in that manner (Art 12.1); and it must be given free of charge (Art. 12.5).[172] Rec. 58 of the GDPR confirms this by stating 'that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used'. Most importantly in the context of this thesis, Rec. 58 adds that 'given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand'. The comprehensibility requirement has been recently explicitly extended to the more general scope of 'vulnerable groups'.[173] Unfortunately, currently many smart products sold to vulnerable individuals do not fulfil GDPR's information conditions. For example, safety and privacy information provided by devices targeting children is often insufficient, not clear and difficult to find.[174]

2.2.I.B Transparent, Concise, Intelligible and Easily Accessible Information

The 'concise and transparent' condition signifies that data controllers have to communicate information 'efficiently and succinctly in order to avoid information fatigue'.[175] This kind of information needs to be clearly separated from information which is not privacy related (for example, contractual provisions). Art. 12.1 of the GDPR states that information should be given in writing (as the default option) but also allows for other 'means' to be used, including electronic means (without specifying which ones but WP29 gives the example of voice alerts,

[172] Ibid.

[173] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (12-13 November 2019) 14 <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf> accessed 1 July 2022.

[174] Sarah Turner, 'Connected Toys: What Device Documentation Explains about Privacy and Security' (*PETRAS*, 2020) <https://discovery.ucl.ac.uk/id/eprint/10100395/7/Turner_PETRAS_Connected-Toys_whitepaper_12062020.pdf> accessed 1 July 2022.

[175] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

cartoons, infographics or flowcharts). If the privacy notice is communicated online, the WP29 recommends using layered privacy statements to make it easier for the data subject to access information on a specific topic instead of needing to scroll through a long document[176]. It adds that data controllers can decide to implement supplementary transparency tools that deliver tailored information to a specific person, taking into consideration the position of this particular individual and the goods or services that he or she uses.[177] Concerning text or visuals, they must 'actually mean something to children' and to adults with cognitive disabilities.[178] To make this happen, researchers suggest using co-design and co-creation methods involving children in the process of writing and testing new techniques of communicating information.[179] The results of such work could be used by policy makers as an element of a code of practice on how to make information more transparent for vulnerable people.

A recurring problem is the unacceptable manner in which updates to privacy policies are communicated to data subjects. This is not a problem just related to the IoT sector. Many companies such as edX, Snapchat or Bloomberg simply label their privacy policies as revised and one needs to accept them with all the modifications they contain.[180] This is not concise and not transparent. Changes to a privacy policy should be communicated separately from the whole privacy policy. How can we expect citizens, not to mention vulnerable people, to identify what has been changed in the new policy compared to the previous one? Lawyers writing those policies track changes and it would not be additional work to specifically communicate to the data subject what has actually changed in the document. Companies developing smart products should take this problem into consideration when modifying their privacy notices.

In terms of the 'easily accessible' requirement, the data subject should not have to search for information and it should be instantly evident where this information can be found.[181] There are

[176] Ibid.
[177] Ibid.
[178] Ingrida and others (n 140).
[179] Veronica Donoso, Maarten Van Mechelen and Valerie Verdoodt, 'Increasing User Empowerment through Participatory and Co-design Methodologies' (*EMSOC*, 2014) <https://www.researchgate.net/publication/298722734_Increasing_User_Empowerment_through_Participatory_and_Co-design_Methodologies_EMSOC_report> accessed 1 July 2022; Ingrida and others (n 140).
[180] Jayashree Mohan, Melissa Wasserman and Vijay Chidambaram, 'Analyzing GDPR Compliance Through the Lens of Privacy Policy' in Vijay Gadepally and others (eds), *Heterogeneous Data Management, Polystores, and Analytics for Healthcare* (Springer International Publishing 2019).
[181] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

various ways to achieve this such as providing information directly to the data subject, clearly signposting it, linking the data subject to relevant information or asking a natural language question ('for example in an online layered privacy statement/notice, in FAQs, by way of contextual pop-ups which activate when a data subject fills in an online form, or in an interactive digital context through a chatbot interface etc.').[182] The WP29 underlines 'push' and 'pull' notices as a useful tool to provide information more transparently. Push notices mean that information is provided 'just-in-time' while pull notices help with getting access to information through, for example, a privacy dashboard, 'learn more' tutorials or permission management tools. These tools give the consumer a more user-centric privacy experience.[183] This seems very relevant to vulnerable people as they will have more difficulties in accessing information. While online layered privacy statements are certainly better than long and illegible privacy policies, it is hard to imagine most people reading through those privacy statements anyway. One useful mechanism that could be implemented would be to identify the most relevant privacy-related information in the context of a product and provide it through the above-mentioned contextual pop-ups or through push notifications (to be effective, the latter would also need to satisfy all the other transparency requirements of being concise, intelligible etc.). For example, a smart home IoT device letting the vulnerable user know through a pop-up that location data is enabled and giving the opportunity to easily disable this feature seems much more useful than including this information only within the privacy notice.

In its 'Opinion on Recent Developments in the Internet of Things', the WP29 proposed scanning QR codes on smart products as a useful way to display information transparently and it has reiterated this in its document related to the transparency principle from 2017.[184] However, this advice proves to be controversial as it seems contrary to WP29's own recommendation that the data subject should not need to take active steps to find information.[185] Smart home products are electronic devices that could communicate with data subjects themselves and there are no technical or economic reasons that would prevent this.[186] Advice to implement QR codes does not seem to be an effective way of helping vulnerable users in accessing and

[182] Ibid.

[183] Ibid.

[184] Article 29 Working Party, 'Opinion 8/2014 on the recent developments on the Internet of Things' (n 37); Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

[185] Ibid. ; Castelluccia and others (n 69).

[186] Ibid.

understanding privacy policies related to their IoT devices. Scanning QR codes would make it more difficult for some vulnerable people to exercise their data protection rights.

Smart devices have their own particular issues that need to be overcome such as the recurring lack of a user interface (which might have led the WP29 to propose the scanning QR codes solution). Indeed, some argue that there is an existing assumption that smart products should not have any physical user interface.[187] Leaving the user alone to look on a website or app where the privacy notice can be found and privacy settings changed could prevent vulnerable individuals, such as elderly people, from being able to choose how their personal data is processed (this is the case, for example, for the Rach.io's Iro and Blossom smart sprinklers).[188] Such design choices do not make information easily accessible. Although it insisted on QR codes, the WP29 also proposed other measures – namely, icons, 'voice alerts, written details incorporated into paper set-up instructions, or videos incorporated into digital set-up instructions, written information on the smart device, messages sent by SMS or email, visible boards containing the information, public signage, public information campaigns'.[189] Delivering a hard copy instruction manual and an URL of a webpage address at which the privacy statement and settings can be consulted is an example of one solution. Providing information orally through audio capabilities of the screenless smart devices could also be an important tool if they have such capabilities[190], especially when oral information is delivered to visually impaired persons or vulnerable people who may have problems in understanding or getting access to written information. How the problem of a lack of user interfaces can be resolved is an important question for a just society as well as for compliance with the GDPR.

The right to receive transparent information and communications forces data controllers to ensure that information is 'intelligible', which signifies that it should be comprehended by an average member of the target audience.[191] The Court of Justice of the European Union (CJEU) confirmed this in the Kásler case by stating that the intelligible and plain language requirements (we will analyse this last term in more detail in point 3.) 'cannot… be reduced merely to their

[187] Galen Gruman, 'IoT Silliness: 'Headless' devices without a UI' (*InfoWorld*, 13 January 2015) <https://www.infoworld.com/article/2867356/beware-this-iot-fallacy-the-headless-device.html> accessed 1 July 2022.

[188] Ibid.

[189] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

[190] Ibid.

[191] Ibid.

being formally and grammatically intelligible', but instead have to be understood in 'a broad sense' taking into consideration an 'average consumer, who is reasonably well informed and reasonably observant and circumspect' and who should have the capacity to 'assess the potentially significant economic consequences for him'.[192] As a consequence, the data controller has to first establish its target audience and find out the average audience member's level of comprehension. A smart device targeted at children might need to present information differently than an IoT product developed for people living with dementia. Moreover, the target audience might in the end turn out different than the actual audience. For this reason, the data controller should regularly control whether its communication mechanisms are still well adapted to the actual audience and modify them if required. This is especially important in the context of vulnerable people and organisations 'should have the flexibility to provide transparency and notices in the way they think is most appropriate'.[193] The WP29 adds that controllers can prove that they comply with the transparency principle by conducting tests on the intelligibility and efficiency of the user interfaces, policies, notices and other means of communicating information through panels accessed by the data subject.[194] Concerning IoT products developed for the general public, this PhD argues in favour of always assuming that they could be used by a child or vulnerable adult and of adapting communication mechanisms accordingly by default. In this way, protection of vulnerable people will increase while organisations will face less compliance-related issues.

2.2.I.C Clear and Plain Language for Vulnerable People

Apart from the concise, transparent, easily accessible and intelligible conditions of providing information to data subjects, the data controller must also ensure that information is provided clearly and in plain language, especially when the data subject is a child.[195] Concerning the plain and clear language requirement, the WP29 calls for the adoption of 'best practices for clear writing' when delivering written information (and when such information is provided orally, by audio or audio-visual methods, including for persons who are visually impaired).[196] In this

[192] Noto La Diega and Walden (n 132); Árpád Kásler v OTP Jelzálogbank Zrt, Case C-26/13, [2014] (ECLI:EU:C:2014:282).

[193] Centre for Information Policy Leadership, 'GDPR Implementation in Respect of Children's Data and Consent' (n 144).

[194] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

[195] GDPR, art 12.1.

[196] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

context, the WP29 recommends to read the European Commission's guide entitled 'How to Write Clearly' from 2011.[197] While the latter provides guidance in terms of how to write clearly for the general audience, outside specialists and EU insiders, it does not mention children or groups of vulnerable people. A paper from a few years ago has underlined the need for further studies to evaluate the most effective ways of providing information to adults with cognitive disabilities in easy-read formats.[198] In the absence of exhaustive and in-depth scientific studies on the effectiveness of easy-read guidelines, organisations should analyse existing choices and adopt those most relevant in the context of their products and needs of children and vulnerable adults.

A comparable language requirement for 'plain, intelligible language' has been employed in EU legislation before and is also used in the context of consent in Rec. 42 of the GDPR.[199] The WP29 underlines that the clear and plain language condition signifies that information should be delivered in 'as simple a manner as possible, avoiding complex sentence and language structures' and that it should be 'concrete and definitive', not 'phrased in abstract or ambivalent terms or leave room for different interpretations'.[200] The purpose and legal basis for processing should be clear. The data controller should not use terms such as 'might', 'may', 'some', 'possible' and 'often'.[201] Sentences and paragraphs should be 'well structured, utilising bullets and indents to signal hierarchical relationships'.[202] The WP29 also requires to use the active and not the passive form, and to avoid using too many nouns. Information delivered to data subjects should not be presented in 'legalistic, technical or specialist language or terminology'.[203] If organisations followed those guidelines, this would help both ordinary citizens and vulnerable individuals.

When a data controller collects children's personal data or when its smart devices could be collecting this type of data (especially when the controller uses the consent legal basis), it not only has to make certain that the style and tone of the language is adapted to children but also

[197] European Commission, 'How to Write Clearly' (*europa.eu*, 2011) <https://op.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5> accessed 1 July 2022.

[198] Rebekah Joy Sutherland and Tom Isherwood, 'The Evidence for Easy-Read for People With Intellectual Disabilities: A Systematic Literature Review' (2016) 13(4) Journal of Policy and Practice in Intellectual Disabilities 297.

[199] Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts [1993] OJ L 95/29.

[200] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

[201] Ibid.

[202] Ibid.

[203] Ibid.

that it resonates with them so that they know that the information is important and that they need to familiarise themselves with it. The WP29 points to the UN Convention on the Rights of the Child as a helpful example of child-oriented language that should be adopted as an alternative to the legal language from the original document.[204] The WP29 also informs that if a data controller knows that their smart devices are used by (or marketed to) other vulnerable groups of people, such as people with cognitive disabilities, the vulnerabilities of those people should be taken into consideration by the data controller when it evaluates how to comply with transparency requirements (in this context, the UN Convention on the Rights of Persons with Disabilities also underlines that relevant support and assistance should be given to people with disabilities so that they can access information as easily as ordinary citizens).[205] This is related to the previously mentioned intelligibility condition, which requires organisations working on smart devices to identify its consumers and audience and adapt its communication mechanisms to their needs.[206] To underline this point again, this thesis considers that all information should be provided in a version adapted to children and vulnerable adults by default as this would help all people in understanding privacy policies and ensure that vulnerable persons are better protected when they use any smart device.

On the one hand, the CJEU, the WP29 and various authors argue that the lack of transparency is a major issue as it makes the use of data subject rights difficult[207]. This is especially important in today's data-driven IoT world where users' profiling is widespread.[208] On the other hand, others underline the complexity of explaining data processing activities in clear and plain language and that this can often result in simple explanations not sufficiently reflecting the actual reality of what is happening to personal data.[209] Some researchers consider that simplifying communications can limit information's quality.[210] However, for others, 'the fact that the information is addressed to a child does not mean that the scope of such notice is

[204] UNICEF, 'UN Convention on the Rights of the Child in Child Friendly Language 2016' (2016) <https://www.unicef.org/sop/convention-rights-child-child-friendly-version> accessed 1 July 2022.

[205] Convention on the Rights of Persons with Disabilities GA Res. 61/106, annex, 61 UN Gaor supp. (No 49) at 65, UN doc. A/61/49 (2006); Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

[206] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

[207] Smaranda Bara and Others v Casa Naţională de Asigurări de Sănătate and Others, Case C-201/14, [2015] (ECLI:EU:C:2015:638).

[208] Nóra Ni Loideain, 'A Port in the Data-Sharing Storm: the GDPR and the Internet of Things' (2019) 4(2) Journal of Cyber Policy 178.

[209] Custers and others (n 168).

[210] Wachter (n 55).

reduced'.[211] This PhD considers that companies could provide a link to the more complicated privacy policy if users desire to read it while focussing the data subject's attention on the simplified version. Easy to understand notices instead of complicated privacy policies 'for adults' would be much more useful for everyone. Many non-vulnerable adults complain that privacy policies are complicated and not understandable. They would benefit from more clarity themselves.

2.2.I.D Increasing Transparency Through Other GDPR Mechanisms

Rec. 39 of the GDPR mentions the importance of raising data subjects' awareness about the risks, rules and safeguards concerning the processing of their personal data.[212] Wachter proposed a three-step transparency model in the context of data protection and the IoT.[213] She argues in favour of openly describing possible risks (1), presenting mechanisms in place to limit those risks (2) and to mitigate them (3). Indeed, a company can never guarantee complete data protection and it should give data subjects truthful information about the risks involved. Risks can be linked to several GDPR provisions. Particularly relevant here are those related to data protection impact assessments (DPIAs). The latter are required if processing is likely to result in high risks for data subjects. Processing vulnerable people's data is one of the criteria for evaluating whether a high risk exists (DPIAs will be analysed in more detail in Section 2.V).[214] Organisations can choose to publish the DPIA or parts of it in order to promote trust in their processing activities and to prove transparency as well as accountability (even if such a publication is not required by law).[215] Even if an IoT developer decides that a DPIA is not necessary, it could publish reasons behind this decision and, therefore, increase the transparency of its practices.[216] This would inform data subjects if a certain product has taken their needs into consideration. How many organisations will actually publish their DPIAs remains to be seen.

[211] Dana Volosevici, 'Child Protection under GDPR' (2019) 6(2) A Journal of Social and Legal Studies 17, 20.

[212] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

[213] Wachter (n 55).

[214] Information Commissioner's Office, 'When do we need to do a DPIA?' (n 11).

[215] Article 29 Working Party, 'Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679' (n 12).

[216] Wachter (n 55).

Adhering to industry codes of conduct (Art. 40 GDPR) can also support the demonstration of transparent data processing.[217] A regulator-led code of practice, the ICO's Age Appropriate Design, has been recently published but it only concerns children. It would be useful to make more references to vulnerable adults in such documents to raise awareness about the need and requirement to take special protection measures also in relation to them. ICO's Age Appropriate Design code could be expanded by the IoT sector by putting forward a new industry-led document related to vulnerable individuals, in line with Art. 40 of the GDPR.

Another pertinent topic concerning transparent communication is data protection by design and by default (Art. 25 GDPR). Those principles are discussed in more detail later in the study (Section 2.IV). They require data controllers to implement data protection measures into their processing activities and devices from the beginning instead of taking data protection into consideration as a last resort compliance solution when problems appear. Rec. 78 affirms that ensuring transparency with regard to the functions and processing of personal data is one of the measures that could help demonstrate compliance with the data protection by design and by default principle. The government is currently developing a labelling scheme for consumer IoT product security.[218] If such a label provides clear information and really proves that organisations have incorporated best cybersecurity practices into their products by design, it could help customers in making more informed choices and raise their awareness about how a specific smart device will protect their personal data.

2.2.I.E Conclusion as to the Relationship Between Transparency, Vulnerable Individuals and Smart Devices

Data controllers have to take into consideration vulnerable people's needs when complying with transparency requirements. The GDPR discusses the necessity of using clear and plain language understandable by a child (or a vulnerable adult). Organisations are obliged to regularly check whether their communication mechanisms are adapted to their audience. Current guidelines propose some measures to satisfy the transparency conditions such as using online layered privacy statements/notices, contextual pop-ups, etc. The WP29 mentions, for

[217] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 83).

[218] DCMS, 'Consultation on the Government's Regulatory Proposals regarding Consumer Internet of Things (IoT) Security' (3 February 2020) <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security> accessed 1 July 2022.

example, the UN Convention of the Rights of the Child as a useful illustration of language oriented towards children.

This thesis considers that organisations should adjust their communication methods to vulnerable people's needs by default. This would facilitate compliance and vulnerable individuals' data protection rights would be better protected (and information more easily understandable for everyone). How to do this will depend on a specific product. Smart devices without a screen might require different measures than those which have one. Moreover, when an organisation produces a device specifically targeted at a particular group of vulnerable people, such as people living with dementia, then it should further adjust their communication mechanisms to their needs.

Finally, transparency alone is not enough to protect users' data. While it is an important element of educating users and supporting them in making informed choices, it is not possible to expect that as long as a data subject is informed, 'they will therefore make rational choices and be able to exercise their rights'.[219] A system where transparent information is provided to the data subject is not sufficient to justify data processing activities. Transparency should work in conjunction with other data protection principles such as fairness and data minimisation, which this thesis will analyse in subsequent sections.

2.2.II Fair Processing of Vulnerable People's Data by Smart Devices

Fairness is an overarching principle that should be considered in all data processing activities (2.2.II.A). It is explicitly mentioned in relation to transparency and is often an implicit requirement to balance the controller's interests against the rights and freedoms of the data subject. The broad scope of fairness gives the opportunity to operationalise ethics in the context of smart devices and other new technologies being used by vulnerable data subjects (2.2.II.B).

2.2.II.A Fairness as an Overarching and Distinct Principle of Data Protection Law

[219] Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' ssrn: 2784123 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123> accessed 1 July 2022.

This thesis will now consider how the principle of fairness should be applied when a data controller develops and deploys smart devices used by vulnerable people. This principle is logically very important in this context as it should ensure that vulnerable persons benefit in the same way from GDPR protections and rights as other citizens. But what does this mean in practice? Is there an intelligible interpretation of this principle that could help organisations in implementing it in the real world?

According to Art. 8 of the Charter of Fundamental Rights of the European Union, 'data must be processed fairly' and on the basis of a 'legitimate basis laid down by law'.[220] Art. 5.1 (a) of the GDPR confirms that personal data has to be 'processed lawfully, fairly and in a transparent manner in relation to the data subject'. Even though this principle is mentioned with two others in one sentence (lawfulness and transparency), whereas other GDPR principles have all their own separate provisions, fairness is a distinct GDPR principle according to Rec. 60 of the GDPR (plural mention of 'the principles of fair and transparent processing…') and legal scholars.[221] Art. 5.1 (a) might mention those principles together simply because of their important interdependence and reciprocal influence, without prejudice to the fact that they are distinct data protection tenets.

Fairness means that people's data must not be 'processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject'.[222] This means, inter alia, that certain data categories are expected to stay private or only be processed in specific circumstances, and that the processing of data should not come as a surprise to data subjects.[223] Fairness is clearly an overarching principle that should be considered during any activity and at every stage of data processing. Considering its objectives, the effective implementation of the fairness principle would support many data subject's rights such as the right to intervene, the right to limit the processing of data and the right to information.[224]

[220] Charter of Fundamental Rights of the European Union (n 67).

[221] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130.

[222] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (n 173).

[223] EDPB, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (n 91).

[224] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (n 173).

The EDPB further clarifies that the principle of fairness signifies 'recognising the reasonable expectations of the data subjects', taking into consideration the possible negative effects that processing may have on the latter, and considering the potential imbalance between the data controller and the data subject.[225] Concerning the term 'reasonable expectations' and vulnerable individuals, the ICO underlines that children 'should be able to expect the service to operate in the way' the service provider has promised that it will.[226] The data controller needs to have appropriate systems in place to implement its own behaviour policies. Data processing will be considered unfair if this is not the case.[227]

Two main dimensions of the fairness principle seem to encompass its meaning and predominate in the current literature.[228] Firstly, data controllers need to take into consideration the consequences of data processing on their customers' rights when choosing and implementing a relevant lawful basis in order to respect the fairness principle.[229] Secondly, processing will only be considered fair if it is transparent.[230] This thesis will now turn to analysing in more detail how data controllers should implement those requirements.

2.2.II.B Various Dimensions of the Fairness Principle

To some authors 'fairness is a subjective, context-dependent and highly politicized concept' and 'a global consensus on what is fair is unlikely to emerge, in the context of algorithmic decision making or otherwise'.[231] To others, 'fairness is a broad criterion which is difficult to explicate exhaustively; it is also context dependent'.[232] While all this may be true, it is important to reflect on how fairness should be applied by data controllers in the context of this study. Organisations need to be guided as subjective interpretations will not help neither with GDPR

[225] EDPB, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (n 91).
[226] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).
[227] Ibid.
[228] Michael Butterworth, 'The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework' (2018) 34(2) Computer Law & Security Review 257; Clifford and Ausloos (n 221).
[229] EDPB, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (n 91).
[230] Information Commissioner's Office, 'Big Data, Artificial Intelligence, Machine Learning and Data Protection' (9 September 2017) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 1 July 2022.
[231] Serge Abiteboul and Julia Stoyanovich, 'Transparency, Fairness, Data Protection, Neutrality' (2019) 11(3) Journal of Data and Information Quality 1, 6.
[232] Buitelaar 306 (n 3).

compliance nor with protecting vulnerable people's rights. The importance of the principle of fairness in the GDPR is evidence of the increasing imbalance of power between the data controller and the data subject.[233] This imbalance of power increases even more when children or vulnerable adults use technology. This thesis will explain what fairness signifies when vulnerable people's data is processed by smart devices from two perspectives. Firstly, there is a clear link between fairness and transparency (2.2.II.B.1). Secondly, fairness requires data controllers to carry out balancing exercises (2.2.II.B.2). Even though in practice these components of fairness function simultaneously, discussing them separately makes it easier to better understand how the fairness principle works within the GDPR.[234] Finally, the section on fairness will be concluded by reflecting on the opportunities and challenges linked to this concept (2.2.II.B.3).

2.2.II.B.1 Fairness Requires Transparency

Despite the fact that fairness is not defined in the GDPR, some scholars, the WP29 and the EDPB have made attempts to do so. They consider that this principle is related to awareness.[235] The fairness principle demands that personal data should only be collected when the data subject is made aware of this processing activity.[236] There is an evident link between transparency and fairness. Apart from Art. 5.1 (a) mentioned above, Art. 13 and Art. 14 of the GDPR also demand 'fair and transparent processing'. In its Age Appropriate Design report, the ICO states that if an organisation is not 'clear, open and honest' about the service it provides and how it functions, then its 'original collection and ongoing use of the child's personal data is unlikely to be fair'.[237] This is crucial for developers of IoT products as those devices gather huge amounts of personal data, sometimes falling into a special category (for example, health tracking devices for vulnerable adults).[238] The seamless data collection operations can make data subjects forget that their personal data is constantly gathered. Sensors of smart devices are designed to be invisible and non-intrusive. Data controllers developing and deploying IoT products need to make sure that individuals 'in the geographical or digital vicinity of connected

[233] Butterworth (n 228).
[234] Clifford and Ausloos (n 221).
[235] Wachter (n 55); Article 29 Working Party, 'Opinion 8/2014 on the recent developments on the Internet of Things' (n 37).
[236] Ibid.
[237] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).
[238] Wachter (n 55).

devices' understand that their data is being collected.[239] Moreover, according to the WP29, fair collection of data represents one of the data subjects' essential expectations concerning IoT devices.[240] Processing is unfair if, for example, a health-related smart product monitors heartbeat data but also gathers blood oxygen levels without appropriately informing the data subject about this through the device's interface or other means.[241] Another example is an IoT device that uses data to make it harder for children (or vulnerable adults) to take a break from using a service or disengage at will. It could be using a vulnerable person's personal data to 'exploit human susceptibility to reward, anticipatory and pleasure-seeking behaviours, or peer pressure'.[242] Such a device would be likely to violate the fairness principle and would be more harmful for vulnerable individuals. It would definitely violate the special GDPR provisions related to children laid out in Rec. 38.

While they are linked, fairness and transparency do not have the same meaning. Fairness seems to be a tool through which transparency should be interpreted (although there are few guidelines on how to do this). This is important in the context of vulnerability. If a smart device provides information transparently to the general population but not to the minority of people with mental disabilities that also use this product, this should not be considered as 'fair transparency'. More broadly, this PhD argues that fair transparency should be viewed as requiring organisations to adopt special data protection measures for vulnerable people by default in any smart product (such as high privacy settings, opt-in mechanisms or child-friendly language to name a few).

In the context of the argument in favour of adopting special data protection measures for vulnerable people by default, there is one other important issue that should be mentioned. Anyone can become vulnerable at any point because of suddenly deteriorating health or other circumstances. Because a smart device is not targeting vulnerable customers does not mean that those persons will not become vulnerable over time. For this reason, always assuming that a smart device might be used by vulnerable individuals would not only protect currently vulnerable consumers of smart products but also those who will become vulnerable in the future. This should also ensure more effective compliance with the fairness principle.

[239] Article 29 Working Party, 'Opinion 8/2014 on the recent developments on the Internet of Things' (n 37).
[240] Ibid.
[241] Ibid.
[242] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).

Even if a data controller is transparent about its data processing activities, 'this does not negate the fact that the inherent asymmetries may inhibit the data subject from exercising their informed autonomous choice in practice'.[243] This thesis will now analyse how the fairness principle is crucial to enable effective balancing of data controllers' activities and data subjects' rights within the data protection field.

2.2.II.B.2 Balancing Vulnerable People's Rights Against Data Controllers' Interests to Ensure Fair Processing

Fairness has a crucial implicit objective to prevent mishandling of data subjects' data by data controllers through balancing exercises (an important element of how the GDPR works in practice). The CJEU's case law explains that fairness does not only concern the risk of deception but also the potential of negative effects of data processing even when there is no intention to deceive by the data controller.[244] The CJEU's judgements directly link the notion of fairness with the principles of proportionality and necessity, and require fair balancing. For example, in the *Promusicae* case, the Court held that 'the protection of the right to intellectual property is a legitimate aim for the processing of communications data (IP addresses) by reference to Article 13 of Directive 95/46/EC which sets out the legitimate aims for limitations to the right to respect for private life with regard to the processing of personal data'.[245] To attain 'fair balance' in the implementation of the GDPR requirements, data processing activities cannot disproportionately disregard data subjects' fundamental rights and freedoms, especially their right of personal data protection.[246] As it has been discussed in Section 1, the legitimate interests and performance of a contract legal bases are examples of provisions requiring data controllers to perform balancing exercises. However, the notion of fairness is overarching and also applies to other principles and data subjects' rights such as the right to object (Art. 21 GDPR) or the right to erasure (Art. 17 GDPR).

[243] Clifford and Ausloos 140 (n 221).

[244] Ibid 141.

[245] Productores de Música de España (Promusicae) v Telefónica de España SAU, Case C-275/06, [2008] (ECLI:EU:C:2008:54).

[246] Clifford and Ausloos 141 (n 221).

A balancing exercise is often implicitly required by the GDPR to be carried out by controllers, as evidenced by academic papers, data protection authorities' guidelines and CJEU's cases.[247] Fair balancing is to be defined and evaluated on a case-by-case basis. It will not and should not be applied in the same way in each situation. As a consequence, data controllers who want to increase their chances of compliance with the GDPR would need to be familiar with relevant case law in their respective sectors (if it exists) and hope that their analysis will be accurate and effective. Although aimed at EU policy makers and legislators, there are guidelines that could be useful such as EDPS's toolkit on 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data' (unfortunately it does not contain any explicit mention of fairness) and EDPS's 'guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' (this document does mention fair balancing).[248]

In the context of the topic of this thesis, relevant guidelines are scarce. Some can be found in ICO's Age Appropriate Design report.[249] If vulnerable people's data is processed by a smart product, data controllers will need to take into consideration an increased power imbalance between themselves and the data subject to ensure that data processing is fair. For example, a smart device sharing children's personal data with a third party would need to be justified by a 'compelling reason to do so, taking account of the best interests of the child' in order for data processing to be fair.[250] Another example is using personal data to support technology features that nudge children towards helpful resources in order to promote their wellbeing and their health. In this situation, the ICO is much more lenient and instead of requiring a 'compelling reason' as in the previous example, simply states that in the presence of a lawful legal basis it is likely that such processing would be fair.[251] Fair processing is context dependent and more examples of fair balancing in the IoT sector would be certainly helpful for data controllers.

[247] Ibid.

[248] EDPS, 'EDPS Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data' (19 December 2019) <https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf> accessed 1 July 2022; EDPS, 'Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (11 April 2017) <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf> accessed 1 July 2022.

[249] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).

[250] Ibid.

[251] Ibid.

2.2.II.B.3 The Current Place of Fairness Within the GPDR – Opportunities and Challenges

The legal academic literature and current guidelines show that fairness is a complicated and often not well understood concept in the data protection field, certainly in the IoT sector. Clifford and Ausloos argue that 'future vague uses of fairness in principle "name-dropping" without a more nuanced understanding' must be avoided.[252] In addition to data protection, fairness is also an essential principle in other legal fields, especially consumer law and competition law. In both the Unfair Terms Directive as well as the Unfair Commercial Practices directive, fairness is incorporated as a standard against which the lawfulness of commercial practices and contractual terms are evaluated.[253] In the competition law context, fairness can be viewed as an intrinsic goal or result of competition enforcement as well as representing 'competition on the merits' (this notion being used to differentiate between restrictive competitive behaviour and lawful practices). Fairness 'can act as a connecting factor to align substantive protections and enforcement mechanisms in the three fields'.[254] Even though the application of the fairness principle is context dependent, best practices and lessons learned from applying this concept in one of the three areas could be a useful source of information on how to implement it in the other two. For example, taking vulnerable people's needs into consideration (in line with GDPR requirements) when carrying out fair balancing exercises in the data protection field would also hopefully lead to similar applications of fairness in other consumer protection areas. In any case, the established interrelation of competition, consumer law and data protection should be further studied to evaluate how it can safeguard and foster vulnerable individuals' rights as well as facilitate legal compliance for organisations developing smart products.

Precisely because clarifications are still needed regarding the meaning of the fairness principle, there is an opportunity to define it more holistically and to go beyond strict legal limitations in order to express more recent data ethics initiatives.[255] According to EU's Agency for Fundamental Rights, the concept of fairness within the GDPR can be considered as requiring data to be processed in an ethical manner and goes beyond the need to provide information

[252] Clifford and Ausloos 187 (n 221).

[253] Inge Graef, Damian Clifford and Peggy Valcke, 'Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law' (2018) 8(3) International Data Privacy Law 200.

[254] Ibid 200.

[255] Clifford and Ausloos (n 221).

transparently to the data subject.[256] The EDPS has called for the EU to reflect urgently on ethics and 'the place for human dignity in the technologies of the future', partly by encouraging a debate on how the fairness principle should be perceived .[257] It is not in the scope of this study to try to answer the question of how ethics and fairness should function together within the GPDR framework. This thesis simply wants to underline an opportunity to develop guidelines on how ethics and fairness can support data subjects' rights (especially those of vulnerable people) and guide controllers in their implementation of GDPR provisions. This raises another question of how to enforce ethics and the principle of fairness in general. Their successful implementation depends on effective enforcement.[258]

This PhD argues that while some guidelines exist (for example, a few examples of what is fair and unfair processing in the ICO's Age Appropriate Design code of practice), more comprehensive explanations related to the fairness principle should be proposed by academics and relevant stakeholders, and then published by relevant authorities. The importance of the fairness principle for vulnerable people's rights, especially in the context of the seamless physical and permanent presence of smart devices within their homes (which increases the power imbalance and makes the latter more likely, real and risky), could make the still not fully entrenched and challenging field of domestic IoT a useful area to start with in terms of the development of more comprehensive guidance. Fairness will certainly continue to require a case-by-case analysis but this does not mean that best practices of complying with this principle should not be published. In the meantime, it is important for IoT organisations not to ignore fairness and consider its impact on all of their data processing activities. This principle will certainly be taken into account by courts and regulators when judging a data controller's compliance with the GDPR.

2.2.III Minimising the Exposure of Vulnerable People to Data Protection Threats

This thesis will now explore the principle of data minimisation and how it relates to vulnerable people's data collected by smart products. While data minimisation can occur any time, what

[256] FRA, 'Handbook on European Data Protection Law' (April 2018) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf> accessed 1 July 2022.

[257] EDPS, 'Opinion 4/2015 Towards a New Digital Ethics' (11 September 2015) <https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf> accessed 1 July 2022.

[258] Graef, Clifford and Valcke (n 253).

is crucial is how it has been implemented before data collection has even started. This is reflected in Art. 25.2 of the GDPR, which states that the controller shall 'implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility'. While the principle of data protection by design and by default is discussed in a separate part of this thesis in more detail, it is important to mention Art. 25 here as well because of its explicit provision regarding data minimisation.

Art. 5.1 (c) of the GDPR states that processing of personal data should be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. Rec. 39 adds that 'this requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means'.Those provisions show that the effective application of the principle of data minimisation is closely linked to the implementation of the purpose limitation (Art. 5.1 (b) GDPR) and storage limitation (Art. 5.1 (e) GDPR) principles as well as to the right to erasure (Art. 17 GDPR) and the right to rectification (Art. 16 GDPR).[259] For example, in the context of storage limitation and profiling, the WP29 recommends to meet the data minimisation requirement by incorporating a clear retention duration for profiles and for data used to create them or to employ them.[260] ENISA observed that data minimisation does not only mean reducing data fields in a form but also refers to any other means of minimising data collection and data processing activities 'following not only a quantitative but also a qualitative approach'.[261] ENISA proposes to minimise data through processes such as 'aggregating, counting, randomising or anonymising personal data, based on a privacy engineering approach'.[262] The right solution will often depend on the context and sector in which a smart device is used.

[259] FRA, 'Handbook on European Data Protection Law' (n 256).
[260] Article 29 Working Party, 'Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679' (n 104).
[261] ENISA, 'Recommendations on Shaping Technology According to GDPR Provisions - Exploring the Notion of Data Protection by Default' (28 January 2018) <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2> accessed 1 July 2022.
[262] Ibid.

In the IoT field, organisations need to ensure that only data that is strictly necessary to provide their services or products is collected. The principle of data minimisation creates a situation opposite to the usual 'data maximalism' linked to smart devices and big data analytics, which relies on extensive data collection and association of data points for better personalisation of services (but is not needed for the core functionality of an IoT product or service).[263] In 2013, the WP29 drew attention to the 'alarming disregard' of the principle of data minimisation in view of the excessive data collection by many apps on smartphones, without any real relationship to the functionality of those apps.[264] As a result of the GDPR, data controllers now need to be ready to prove that they comply with relevant data minimisation best practices and requirements in line with the accountability principle.[265] The less data is processed by a smart device, the less risks and data protection compliance issues an organisation and a vulnerable person will incur. This is of course also true for ordinary citizens. However, considering that vulnerable people's data often falls under a special category and that processing of their data usually involves higher risks, the data minimisation principle grows in importance in this context. IoT products such as connected toys need to integrate into their design GDPR principles, including data minimisation.[266]

In the specific context of smart products used by vulnerable people, one especially relevant problem is when organisations providing information society services (ISS) record and gather personal data to identify the data subject's age in order to know whether they need to obtain consent from a legally authorised representative before they process their personal data (Art. 8 of the GDPR, see Section 1.II.B of this thesis for more details about ISS). Data controllers are required to comply with the principle of data minimisation in this context too.[267] To do so, they will have to gather only the amount of personal data that is strictly necessary to inform them about the age of particular users. This data must only be used for the purpose of providing age appropriate settings and measures and not for any other purpose such as advertising (unless consent has been obtained to do so or another legal basis permits this). The Centre for Information Policy Leadership considered three ways through which a data controller could

[263] Wachter 271 (n 55).

[264] Article 29 Working Party, 'Opinion 02/2013 on Apps on Smart Devices' (WP 202, 2013).

[265] Information Commissioner's Office, 'Principle (c): Data minimisation ' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> accessed 1 July 2022.

[266] Ingrida and others (n 140).

[267] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).

verify a customer's age. It declared that universal age assessment would be too intrusive while verifying the age of data subjects only when services explicitly state that they target children would be under-inclusive. As a consequence, the Centre argued in favour of performing a risk analysis by evaluating 'whether the offering is intentionally made to be attractive to children; whether children have been attracted to the ISS or similar services in the past; and whether the registration process to the ISS reflects an assumption that the users are above the age of digital consent'.[268] This thesis does not consider this approach as appropriate. Firstly, children might be attracted to services that are not designed to be used by them and this would be difficult to verify. Secondly, it seems unrealistic to expect organisations to carry out another risk analysis, especially smaller ones, which already struggle with GDPR compliance. As a result, this PhD argues in favour of minimising data collection through age verification mechanisms that use the best privacy-preserving technologies available, to promote the use of such technologies and develop guides on how to implement them. The ICO recognises that 'there is a tension between age assurance and compliance with the GDPR' because of the 'intrusive data collection' that may take place to obtain age-related data by IoT devices and that age-assurance tools remain a field in early stages of development.[269] It also proposes to use privacy by design solutions to counter this risk and affirmed its support to standardisation and certification mechanisms to help children and their parents in finding age-assurance services that comply with data protection provisions. Best practices should be developed. For example, a smart product should ask for a person's age without storing and keeping their actual date of birth. Once the person confirms that they are over a certain age limit, they would be able to proceed and their data would be automatically deleted. The WP29 advises to reduce the amount of data collected to the minimum necessary to perform a specific service (for example, when the objective can be achieved through aggregated data, developers should not use raw data).[270] Of course, age verification is not the only issue that needs to be reflected upon in the context of data minimisation when vulnerable people use smart products. Another one could be the need to identify the legally authorised representative to give consent on behalf of a child or on behalf of a vulnerable adult. Privacy enhancing technologies could help here as well and this PhD will analyse them in more detail in the fourth chapter of this thesis.

[268] Centre for Information Policy Leadership, 'GDPR Implementation in Respect of Children's Data and Consent' (n 144).

[269] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' 35 (n 26).

[270] Article 29 Working Party, 'Opinion 8/2014 on the recent developments on the Internet of Things' (n 37).

Should the principle of data minimisation be applied differently when vulnerable people use smart products? In its guidelines on apps – which can be applied to smart devices and their interfaces (often controlled by apps) – the WP29 declared that when consent can be lawfully given by a minor, and when the app is meant to be used by a minor, the data controller should take into consideration the latter's potentially restricted comprehension of and interest in information about data processing.[271] As a consequence of their general vulnerability, and in line with the lawfulness and fairness principles, organisations targeting children with their smart products 'should even more strictly respect the principles of data minimisation and purpose limitation'.[272] This means that they should not collect data for the purpose of behavioural advertising (directly or indirectly) as this would not fall within the scope of a minor's comprehension and, therefore, go beyond the lines of lawful processing. This guidance would also apply to IoT products meant to be used by vulnerable adults.

Minimising data collection should have a strong appeal for organisations. The fewer personal data is accessed and processed the less risks an organisation has to face.[273] For this reason, edge computing architectures (as opposed to cloud architectures) might be the future of less invasive data processing that facilitates compliance. As mentioned above, this PhD will explain why and discuss privacy enhancing technologies and architectures on which they are based in-depth in its fourth chapter.

2.2.IV Thinking About Vulnerable People's Data Protection Throughout the Development and Deployment Process of Smart Products

Firstly, data protection by design and by default is briefly defined and discussed in the context of vulnerable people and smart homes (2.2.IV.A). Subsequently, this work focusses on data protection by design, mentions the current main paradigmatic approaches (2.2.IV.B) and discusses how data protection by default should function in smart homes (2.2.IV.C).

2.2.IV.A Defining Data Protection by Design and by Default

[271] Article 29 Working Party, 'Opinion 02/2013 on Apps on Smart Devices' (n 264).

[272] Ibid.

[273] Lachlan Urquhart, 'Towards User Centric Regulation: Exploring the Interface Between Information Technology Law and Human Computer Interaction' (DPhil, University of Nottingham 2017).

Data Protection by Design and by Default (DPbDD) is not a new concept but rather an adaptation of privacy by design, the latter being discussed in scientific papers since the early 2000s and officially used and defined by, for example, the Canadian Privacy Commissioner Ann Cavoukian in 2009.[274] The most important change is that while before privacy by design was a matter of best practices, DPbDD is now a legal obligation under the GDPR. It is also important to underline that privacy and data protection are distinct, although to a certain degree overlapping, fundamental rights listed in Art. 7 and Art. 8 of the Charter of Fundamental Rights of the European Union.[275] DPbDD is specifically related to data protection requirements and not to the broader notion of privacy. This has been 'a wise decision, also because privacy is an open and essentially contested concept, and it would be very difficult to define which design actually protects privacy'.[276] Art. 25 of the GDPR states that:

> 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, *both at the time of the determination of the means for processing and at the time of the processing itself*, implement *appropriate technical and organisational measures*, such as pseudonymization, which are *designed to implement data-protection principles*, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
> 2. The controller shall *implement appropriate technical and organizational measures* for ensuring that, *by default*, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
> […] (emphasis added)

[274] Ann Cavoukian, *Privacy by Design, Take the Challenge* (IPC Business Press 2009); See, e.g., Julie E. Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52(5) Stanford Law Review 1373.
[275] Charter of Fundamental Rights of the European Union (n 67).
[276] Mireille Hildebrandt and Laura Tielemans, 'Data Protection by Design and Technology Neutral Law' (2013) 29(5) Computer Law & Security Review 509, 517.

The fundamental obligation set forth in Art. 25 of the GDPR is the effective implementation of GDPR principles and the rights of data subjects by design and by default.[277] In summary, the GDPR introduces a qualified responsibility on data controllers to use technical and organisational measures, which are designed to make certain that personal data processing is compliant with GDPR's provisions and to ensure that consumers' data protection rights are safeguarded. This duty also concerns the default implementation of data protection principles and default boundaries on who has access to personal data.[278] Apart from other considerations (costs, state of the art and the scope, nature, context and purposes of processing), data controllers need to evaluate the risks of varying likelihood and severity for the rights and freedoms of natural persons caused by data processing. In the context of this thesis, when deciding what kind of safeguards and technical and organisational measures need to be taken, data controllers should evaluate risks posed to vulnerable people's data when the latter use smart devices.

Thinking about vulnerable people's data protection needs does not only concern data controllers as 'every stakeholder in the IoT should apply the principles of Privacy by Design and Privacy by Default'.[279] This becomes particularly true in the context of Rec. 78 of the GDPR, which states that producers of products, services and applications 'should be encouraged to take into account the right to data protection when developing and designing such products, services and applications' to support data controllers in fulfilling their obligations. Rec. 78 encourages producers to take DPbDD measures as those will be 'taken into consideration in the context of public tenders'. As a consequence, if producers of IoT devices invest in privacy by design and by default and, as a result, improve children's and vulnerable adults' data protection, they will have a higher chance in procurement processes. As to data controllers, their choice of a producer of a smart device could facilitate, or on the contrary undermine, their GDPR compliance efforts.

The notion of data protection by design and by default is crucial in the context of vulnerable persons. They have less capacities to defend themselves against security threats or to understand what kind of personal data is processed and for what purposes. Protecting data by

[277] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (n 173).
[278] Lee A. Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4(2) Oslo Law Review 105.
[279] Article 29 Working Party, 'Opinion 8/2014 on the recent developments on the Internet of Things' (n 37).

design and by default can contribute to remediate those issues.[280] The GDPR establishes new requirements that demand organisations to include data protection considerations into all aspects of their processing activities.[281] This DPbDD approach reflects GDPR's risk-based and accountability focus. EDPB's guidelines on data protection by design and by default confirm that this is an overarching principle.[282] Indeed, it discusses transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation as well as integrity and confidentiality, all in the context of how DPbDD can contribute to the implementation of those principles. The GDPR in Rec. 78 mentions, for example, transparency enhancing measures alongside security or data minimisation mechanisms in the context of the implementation of DPbDD.

2.2.IV.B The Need to Consider all GDPR Principles within Data Protection by Design

In terms of vulnerable people and data protection by design, the EDPB explicitly underlines the importance of non-exploitation of 'the needs or vulnerabilities' of data subjects (fairness) and of the comprehensibility of data processing, especially when the data subjects are children or vulnerable adults (transparency).[283] Vulnerable people's data protection needs should be taken into account when designing smart devices. However, what should be prioritised? Data protection by design quite clearly requires data controllers to take into consideration all GDPR principles. While there are different paradigmatic approaches to implementing the data protection by design principle, current technologies seem to focus on confidentiality and are often criticised for doing so.[284] What should be the approach adopted in the specific context of vulnerable individuals who live in smart homes? Which paradigmatic approach would be the most appropriate? This will be discussed in more detail in Chapter 3 (from the perspective of professionals) and Chapter 4 (in the context of theoretical legal discussions).

Data protection by design is also essential in the context of transparency. Organisations should inform data subjects about the level of protection that their data will receive (there will always

[280] Bygrave (n 278).

[281] Information Commissioner's Office, 'Data Protection by Design and Default' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> accessed 1 July 2022.

[282] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (n 173).

[283] Ibid.

[284] Veale, Binns and Ausloos (n 117).

be capable adversaries and no data protection system is perfect).[285] Data controllers must communicate to their users that data protection risks will continue to exist, even under the best conditions (unless no personal data is processed), in line with the principle of transparency. Companies need to inform users about the measures they have in place in case their devices are attacked and how their data-related technologies will protect personal data. This will help vulnerable people and their legally authorised representatives in making informed choices as to the company from which they will buy IoT devices. A robust privacy by design strategy can become a selling point to potential consumers.[286] The greater the user's trust is, the higher the chance that they will buy products from a particular company. As a result, comprehensive communication concerning privacy by design measures can be of benefit both to the data controller and to the data subject.

The GDPR gives an opportunity to increase data subjects' data protection. Data protection by design requires an iterative collaborative and inter-disciplinary effort of lawyers, researchers, designers of technologies, supervisory authorities and other stakeholders, to identify and implement the best practices possible. Indeed, 'the lack of a holistic approach for engineering and promoting privacy technologies is certainly one reason for the unsatisfactory status of their maturity and their market availability'.[287] How to implement data protection by design in the context of children and other vulnerable individuals could be the topic of one of those collaborative ventures. Just as the GDPR did at a broader level, solutions and conclusions from such initiatives could have an impact beyond the UK and the EU and promote data protection globally.

2.2.IV.C Protecting Vulnerable People's Data by Default

Standard settings are crucial when evaluating the level of privacy offered by particular IoT devices as they determine how easy it is for users to apply the relevant configuration for a data protection compliant use of the product.[288] Organisations should offer a data protection

[285] Wachter (n 55).
[286] Ibid.
[287] Marit Hansen, 'Data Protection by Design and by Default à la European General Data Protection Regulation' in Anja Lehmann and others (eds), *Privacy and Identity Management Facing up to Next Steps* (Springer International Publishing 2016) 11.
[288] Marit Hansen, 'Data Protection by Default in Identity-Related Applications' (Policies and Research in Identity Management, Third IFIP WG 116 Working Conference, IDMAN 2013, London, April 2013).

compliant product from the moment it is turned on – that is a product where the basic functionalities are turned on by default and only personal data required to provide the latter is collected. The European Data Protection Supervisor declared back in 2012 that the objective of the data protection by default principle is to defend the data subject in situations where there might be a lack of comprehension or control of data processing, in particular in the context of new technologies. The reason this principle exists is to limit the privacy intrusive characteristics of a specific product to what is necessary for simply using it. It should be up to the data subject to decide whether they want to allow their personal data to be used in a broader manner.[289] This proves the importance of data protection by default for vulnerable individuals. Vulnerable individuals might lack understanding or not be able to exercise informed control over their personal data. This is confirmed in Rec. 58 of the GDPR, which states that the justification for the protection of children is founded on their diminished capability of understanding.[290] There are important gaps in the development of children in terms of their comprehension of the digital environment in which their personal data is processed.[291] For example, in the case of persons aged 16-17, the UK's Information Commissioner's Office suggests to 'provide written, video or audio materials to explain what will happen to their information and any associated risks' if they attempt to change a default high privacy setting and to check with an adult if they have any concerns or don't understand what is being communicated to them.[292] ICO's report indicates how important those default settings are. It is absolutely crucial that data processing is left to the choice of each individual as much as possible. Unfortunately, this is not the reality at the moment and many IoT devices continue to transfer personal data to third-parties without even informing the data subject about these activities.[293]

This PhD argues in favour of adopting explicit opt-in mechanisms always and for everyone instead of differentiating between ordinary citizens and children or vulnerable adults. In its

[289] EDPS, 'European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the Data Protection Reform Package' (7 March 2012) <https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf> accessed 1 July 2022.

[290] Malgieri and Niklas (n 19).

[291] Eva Lievens and Simone van der Hof, 'The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR' (2018) Communications Law 33.

[292] ICO, 'Age Appropriate Design: a Code of Practice for Online Services' 42 (n 26).

[293] Jingjing Ren and others, 'Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach' (IMC '19: Proceedings of the Internet Measurement Conference, Amsterdam, October 2019).

Age Appropriate Design report, the ICO requires organisations to adopt 'high privacy' by default, to switch geolocation and profiling off by default 'unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child'.[294] Some authors also stated that in the case of minors using a service, 'default settings have to be especially strict'.[295] This is problematic for several reasons. Firstly, organisations could argue that because their smart products are directed towards the general population, their default settings do not have to be as protective as for products that only children use. Adopting 'high privacy' default settings by default for everyone would not only make all citizens' data safer, but also make sure that when it is uncertain whether a product is used by children (or vulnerable adults), default privacy settings would protect them anyway in case they are using it or decide to use it later. Secondly, the ICO mentions compelling reasons for a different default setting than a high privacy one, without giving examples of what could justify deviating from the GDPR provisions and spirit. This thesis argues in favour of making no such exceptions. Until proven to the contrary, it is difficult to envisage a situation in which a high privacy default setting should not apply. Thirdly, and this is relevant to the first two points, the ICO states itself that a lot of children will simply 'accept whatever default settings you provide and never change their privacy settings'.[296] This PhD argues that this will also be certainly true in many cases for vulnerable adults, especially considering that some reports suggest people in general are reticent to actively change settings which are privacy friendly by default. According to a report from analytics firm Flurry, for example, only 11% of users worldwide have decided to opt into app tracking since the release of the App Tracking Transparency feature with iOS 14.5.[297] For this reason, it is of utmost importance to implement high privacy settings by default for everyone to make sure that all vulnerable individuals are protected. Ordinary citizens would benefit from such an approach as well. Moreover, making individuals change their privacy settings if they want their data to be processed for a specific purpose would also educate them about personal data processing in the IoT world (as they would need to take active steps and think about their choices), thereby contributing to compliance with other GDPR provisions such as the transparency principle.

[294] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).

[295] Hansen, 'Data Protection by Default in Identity-Related Applications' 12 (n 288).

[296] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).

[297] Joe Wituschek, '96% of iPhone Users have Opted Out of App Tracking Since iOS 14.5 Launched' (*iMore*, 6 May 2021) <https://www.imore.com/96-iphone-users-have-opted-out-app-tracking-ios-145-launched> accessed 1 July 2022.

Currently, advice on how to implement data protection by default is scarce so it is important for relevant authorities to lead the way and establish the best solutions possible through their guidelines, provisions and codes of conduct.[298] Data protection by default can 'ruffle the feathers of established Internet business models'.[299] For example, according to Art. 25.2 of the GDPR, tracking a data subject using their personal data would need to be turned off as a default setting. This could have an impact on the well-known business model of paying for a service through personal data without giving the user any choice in this regard. It could seem as if this only concerns websites such as Facebook. However, recently, an extensive and important study on how IoT devices process our data has revealed that personal data gathered by many smart home products (such as smart TVs or cameras) is transferred to various third-party companies (especially Google, Amazon and Akamai concerning devices analysed in this paper), which would give them the possibility to profile data subjects.[300] Those third parties can not only acquire knowledge about the kinds of IoT devices used within a smart home, but also in what manner and at what times they are used, merely through an analysis of the network traffic from the smart products to the cloud services. TVs accounted for the most important part of third-party communications. The study showed that a smart camera transferred data to 52 different IP addresses and a Samsung TV to 30 IP destinations, many of those contact points being not only cloud computing providers but also marketing companies.[301] Some devices, such as the Amazon Ring doorbell, recorded videos of the data subject every time they moved in front of the device without warning the latter, the only information about this function of the device being the fine print in Amazon's privacy policy without any option to turn it off.[302] This is a blatant violation of users' data protection rights. It is not only contrary to the data protection by default principle, but also, for example, the principle of transparency or data minimisation. IoT devices such as smart TVs, doorbells or cameras will certainly be used by children or vulnerable adults in their smart homes and the situations described above are unacceptable. Those practices are disregarding the principle of data protection by default and companies at their origin should be held accountable.

[298] Hansen, 'Data Protection by Design and by Default à la European General Data Protection Regulation' (n 287).
[299] Ibid 11.
[300] Ren and others (n 293).
[301] Ibid.
[302] Ibid.

Finally, as it has been mentioned in Section 2.I on the transparency principle, IoT devices often lack user interfaces and changing settings or even knowing what those settings are is usually complicated and cumbersome for data subjects (especially for vulnerable people). As a result, the implementation of data protection by default becomes even more essential to ensure the protection of vulnerable people's data in smart homes.

2.2.V High Risks of Processing Vulnerable People's Data and DPIAs

DPIAs are an important element of the obligations of an organisation developing or deploying IoT devices used by vulnerable individuals (2.2.V.A). DPIAs are a concept that encourages organisations to self-regulate while also trying to hold them accountable for this self-regulation (2.2.V.B). How exactly should they be implemented remains an open question. In line with the spirit of the GDPR and its provisions, this PhD considers that DPIAs should not only evaluate risks to data protection rights but also social, ethical and human rights (2.2.V.C).

2.2.V.A DPIAs as Essential Elements of Compliance and Protection of Vulnerable Individuals

A data protection impact assessment's (DPIA) objective is to evaluate, identify and minimise risks related to a data processing activity before the latter takes place. It is an essential part of an organisation's accountability obligations, and when conducted in the right manner, can support data controllers in proving that they comply with the GDPR.[303] DPIAs are inclusive and comprehensive processes as they take into consideration all GDPR obligations and principles, and they have a proactive nature because their aim is to prevent data protection issues from materialising instead of acting after the problems have appeared.[304] Because DPIAs require organisations to reflect on risks before the processing takes place, they help in complying with the data protection by design and by default principle. They also support GDPR compliance more broadly as they are a useful way of evaluating and proving compliance with other principles and obligations. They can also contribute to cost reduction as identifying problems early can prevent unnecessary damage. DPIAs seem particularly important when vulnerable people are concerned because they can help an organisation better understand their

[303] Crabtree and others (n 165).

[304] Katerina Demetzou, 'Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of 'High Risk' in the General Data Protection Regulation' (2019) 35(6) Computer Law & Security Review 105342.

expectations and needs. Not carrying out a DPIA when this is required could lead to enforcement action and a fine of up to €10 million or 2% of the global annual turnover whichever is higher.[305] Organisations can use DPIAs carried out by other companies to inform their own DPIAs when relevant – for example, a company deploying a smart product can get inspiration from the DPIA conducted previously by the product developer.[306] Rec. 84 of the GDPR states that 'the outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation'. A DPIA is an on-going process and not a one-off exercise. For example, when an organisation makes important changes to how it processes its customers' data, a new DPIA should be conducted.

DPIAs can be perceived as an element of a larger influence of risk-based processes in the data protection law field.[307] The GDPR does not define the term 'risk' but its provisions explain that it concerns risks to individuals' interests.[308] According to Art. 35.1 of the GDPR, a DPIA is required when a specific processing plan or project is likely to cause a high risk to the rights and freedoms of individuals. Rec. 75 GDPR links risks to the possible harm or damage that could be caused to a person. Risks need to be evaluated to determine their potential for any important physical, material or non-material harm.[309] What needs to be considered is both the severity and likelihood of any possible harm to individuals. While risks suggest a 'more than remote chance of some harm', high risk 'implies a higher threshold', either as a result of the higher likelihood of the harm or because the harm would be more severe, or a mix of the two.[310] The main issue during initial analyses is to decide whether a particular processing operation involves high risks.

The question is not whether high risks actually exist (a DPIA will need to evaluate this) but rather whether there is potential for a high risk. Firstly, it is worth mentioning that if a type of processing activity is not mentioned as necessitating a DPIA in the GDPR, in the ICO's

[305] Information Commissioner's Office, 'What is a DPIA?' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/> accessed 1 July 2022.

[306] Ibid.

[307] David Wright and others, 'Precaution and Privacy Impact Assessment as Modes Towards Risk Governance' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Field* (European Commission 2011).

[308] Information Commissioner's Office, 'What is a DPIA?' (n 305).

[309] Information Commissioner's Office, 'When do we need to do a DPIA?' (n 11).

[310] Ibid.

documents or in European guidelines, then the organisation will need to decide on its own whether an impact assessment should be carried out. If there is any uncertainty, the ICO encourages to do a DPIA to 'ensure compliance and encourage best practice'.[311] Art. 35.3 describes three cases in which a DPIA is always required ('systematic and extensive profiling with significant effects', 'large scale use of sensitive data', 'public monitoring') and the ICO published a document in line with Art. 35.4 listing 10 more examples.[312] Some activities among the latter require a DPIA automatically while others need to occur in combination with one of the criteria in the European guidelines (the WP29 lists 9 other criteria). Processing activities on the basis of data gathered by innovative technologies is one of ICO's criteria that needs to be combined with one of those listed by the WP29. Therefore, the first question in the context of this PhD is whether smart devices can be considered as innovative technologies. Rec. 91 mentions innovative technologies as developments in the technological field globally. The ICO considers that smart technologies (including wearables) fall into this definition.[313] As a result, IoT products fall into the 'innovative technologies' criteria of the ICO. The second question is whether this can be combined with one of WP29's examples of situations likely to result in a high risk. For the WP29, processing data of vulnerable people is an indication that there could be a high risk involved. There is an inherent high risk when vulnerable data subjects' data is processed as there is a power imbalance between the latter and the data controllers, in the sense that vulnerable people (such as children or vulnerable adults) might be incapable of easily consenting or objecting to the processing of their data, or exercising their rights.[314] In conclusion, smart devices (ICO's innovative technology criteria) used by vulnerable people (WP29's processing of vulnerable people's data criteria) represent a situation that might result in high risks and, therefore, a DPIA will always need to be carried out.

A DPIA will need to evaluate 'the origin, nature, particularity and severity' of the risks (Rec. 84). During their evaluation of data processing risks, organisations should remember that decisions that might have little consequences generally could still significantly impact vulnerable adults, children or other vulnerable groups of society.[315][316] Identifying the risks

[311] Ibid.
[312] Ibid.
[313] Ibid.
[314] Article 29 Working Party, 'Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679' (n 12).
[315] Article 29 Working Party, 'Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679' (n 104).
[316] Information Commissioner's Office, 'When do we need to do a DPIA?' (n 11).

involved with data processing is a complex multidisciplinary duty that can be supported by stakeholders as well as citizens.[317] The next section will analyse this in more detail.

2.2.V.B The Meta-Regulation of Organisations through DPIAs

DPIAs were not always mandatory. The obligation to carry out DPIAs in certain circumstances has been introduced by the GDPR. Obligatory impact assessments are not purely prescriptive legal regulations but rather a mix of legal requirements as well as policies that organisations need to develop and implement themselves (with the involvement of relevant stakeholders).[318] Binns has described the term 'co-regulatory' as inadequate and lacking precision in defining what DPIAs are.[319] Instead, he proposes to use the notion of 'meta-regulation' developed by Christine Parker.[320] This concept describes governmental efforts to make companies accountable for their self-regulation attempts. The benefit of meta-regulation in comparison to other types of regulation is that it takes advantage of the organisations' capacity to self-management, but includes mechanisms to verify whether they meet the regulator's expectations. Organisations might be required to analyse and report on their self-regulation plans so that regulators can establish if conditions are being fulfilled. Meta-regulation is composed of legal regulation with an important emphasis on organisations developing their own processes as well. Binns considers meta-regulation as a promising approach, which appears 'to be designed to leverage regulatees' capacity' and 'attempts to allow room for data controllers to apply their own expertise to a problem'.[321] Data controllers do not need to implement a set of specific safeguards and mechanisms but rather find their own effective solutions to reduce risks to fundamental freedoms and rights of data subjects.

Data protection authorities (DPAs) might have a more profound knowledge of data protection provisions but they may not have a better comprehension of the newest data processing methods or privacy-enhancing technologies in a particular sector. Certain situations might

[317] Niels Van Dijk, Raphaël Gellert and Kjetil Rommetveit, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32(2) Computer Law & Security Review 286.
[318] Reuben Binns, 'Data Protection Impact Assessments: a Meta-Regulatory Approach' (2017) 7(1) International Data Privacy Law 22.
[319] Ibid.
[320] Christine Parker, 'Meta-regulation: Legal Accountability for Corporate Social Responsibility' in Doreen McBarnet, Aurora Voiculescu and Tom Campbell (eds), *The New Corporate Accountability: Corporate Social Responsibility and the Law*, vol 29 (CUP 2007).
[321] Binns 32 (n 318).

require specific data protection techniques to reduce risks that only data controllers developing and deploying those devices know about in-depth. Moreover, some organisations working on IoT products targeted at a particular category of vulnerable people will also have a superior understanding of the latter's needs. For this reason, allowing organisations to find their own solutions to the risks involved in their data processing activities makes sense (of course in the framework of relevant GDPR provisions). However, the effectiveness of DPIAs' meta-regulation approach will also be contingent on the ability of DPAs to examine organisations' risk reduction plans. The GDPR empowers them to do so. Art. 36.1 states that 'the controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Art. 35 indicates that the processing would result in a high risk'. The authority could then restrict or proscribe the controller's project if it discovers that 'the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk' (Art. 36.2 GDPR). The requirement to be scrutinised by a supervisory authority does not mean that the latter will be capable of doing this effectively (partly because of their possible lack of expertise in certain domains). In this regard, European Data Protection Board guidance on how to evaluate risk management and mitigation plans would be valuable as it could support supervisory authorities in their evaluation processes.[322] Moreover, risk mitigation and prevention could be different depending on the data subject's identity, sector and technology used to process their data. Building regulators' and DPAs' expertise on issues such as how to evaluate DPIAs when children's or vulnerable adults' data is processed could be an important step towards increased compliance and data protection. This thesis will critically analyse in more depth how DPIAs should be viewed and propose an overarching risk assessment model in the next section 2.2.V.C.

Finally, stakeholder involvement is an essential part of successful meta-regulation. The GDPR reflects this. Art. 35.9 states that 'where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations'. Time will tell how effective this provision will be, especially because of the wording 'where appropriate'.[323] The weakening of this essential GDPR provision in the final version of the regulation has been

[322] Ibid.
[323] Ibid 33.

criticised in legal literature.[324] As a consequence, official guidance on what 'where appropriate' more precisely signifies could have an important effect on organisations' decisions as to who needs to be consulted in a particular situation. For example, in the case of smart devices specifically designed for people living with dementia, it would seem appropriate to consult this group of vulnerable individuals or their carers during the DPIA process. There are no specific mechanisms in the GDPR that would ensure that stakeholders are actually included in data controllers' plans. In the case of vulnerable individuals using smart devices, supervisory authorities might need to evaluate the DPIA (because there could be high risks involved as established previously) and could suggest to take data subjects' or their legal guardians' inputs into consideration. However, there is no guarantee that this will actually happen. Another issue regarding stakeholder participation is that no document explains how such participation should take place, what methods should be adopted and who exactly should participate in the consultations.[325] One paper points to a DPIA template concerning smart grids in which public participation seems to have been undermined in comparison to the text of the GDPR. The authors consider this as 'part of a worrying trend to cancel out the views of the data subject within data protection in general'.[326] The confusion as to what are the general rules and expectations regarding stakeholder involvement should be avoided in the future through more specific guidance which, in the view of this thesis, should foster participation of data subjects and their legally authorised representatives in DPIAs, especially when a smart device is targeting a particular category of vulnerable individuals as it could increase the understanding of how they are affected by data protection issues and enable a stronger protection of their fundamental rights and freedoms. This could be done through a code of conduct or guidelines promoted, for example, by the European Commission with the use of its implementing powers in accordance with Art. 40 of the GDPR.

2.2.V.C Identifying an Ethical Risk Assessment Model

Data protection impact assessments have become mandatory in many cases and, since the entry into force of the GDPR, they are increasingly important in the data protection field. They are of great importance in the context of this thesis as processing vulnerable people's personal data by IoT devices might involve high risks and, therefore, it will require a DPIA. What should

[324] Veale, Binns and Ausloos (n 117).

[325] Van Dijk, Gellert and Rommetveit (n 317).

[326] Ibid 298.

DPIAs take into consideration when evaluating the potential impact of data processing in the context of smart devices used by vulnerable people? Should impact assessments be specific to a particular sector or general? Should they be specific to the nature of the technology? Currently, there is no consensus, neither in theory nor in practice, on how to comprehend the concept of a risk to a right in DPIAs.[327] The DPIA 'involves evaluation of intangible values and comprehensive balancing exercises, including of value conflicts, and consideration of many factors, whether it may lead to unfair discrimination or any other negative impact on the individuals concerned or on society', which might be difficult for organisations to do effectively.[328] As mentioned previously, it is good that organisations have some flexibility in terms of how to carry out DPIAs. However, they also need guidance in terms of the overarching principles of how a DPIA should be conducted. The publication of general guidelines would certainly help data controllers with compliance issues. In this context, the ICO has recently published a DPIA template to be used by organisations providing online services likely to be accessed by children.[329] This template has been adapted from ICO's more general DPIA template. If designed correctly, this kind of document can help organisations in carrying out more effective DPIAs. However, what is this overarching model of risk assessment that organisations should use?

This part of the thesis argues in favour of and is inspired by the 'rights-based and values-oriented model' proposed by Mantelero, which focusses on different application domains (such as crime prevention or healthcare) as well as various groups of rights, values and freedoms instead of the technology.[330] One IoT device might have a completely different method of gathering data than another smart product (for example, one might gather visual data and store it on cloud servers in a third country while another might gather only voice data and store it on the device locally). So, of course, the type of technology used still has significance in the impact assessment process as a particular technology influences the choice of the most appropriate measures to be adopted to safeguard citizens' rights and values. However, what really counts is how individuals' rights and values are preserved in different contexts by the data controller.[331]

[327] Ibid.

[328] Maria Eduarda Gonçalves, 'The Risk-Based Approach Under the New EU Data Protection Regulation: a Critical Perspective' (2020) 23(2) Journal of Risk Research 139, 144.

[329] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26).

[330] Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34(4) Computer Law & Security Review 754, 755.

[331] Ibid.

When a child (or vulnerable adult) uses an IoT device or is subject to big data analytics, it is not the type of the technology as such that should influence the DPIA but rather the fact that it is a child that uses it, and the latter's rights and values. DPIAs should also distinguish in which sector the smart device is being used. If a child uses an IoT product at home for entertainment or a smart device in a hospital for health-related reasons, these are very different settings and so the rights and values will differ as well. For example, in a healthcare environment, freedom of choice or the no-harm principle might be crucial while in a smart city, equal treatment or civic engagement could be the prevailing values.[332] Different circumstances are associated with different values that should be taken into consideration as a point of reference for impact assessments.

For Mantelero, conducting value-oriented impact assessments results in the necessity to shift focus to the 'ethical and social consequences of data processing' and 'the potential negative outcomes on a variety of fundamental rights and principles'.[333] This approach is actually more in line with GDPR's provisions than if DPIAs focus solely on GDPR principles. While the respect of the latter is essential, taking into consideration ethical questions too (such as how a smart health product will impact fundamental rights of a person living with dementia) would better reflect the spirit of the regulation. Indeed, Rec. 75 of the GDPR, for example, mentions discrimination or significant economic or social disadvantages as risks that could result from data processing activities. Both the WP29 and the EDPS have proposed a larger impact assessment encompassing ethical questions and social consequences of data processing.[334] It would seem that DPIA templates taking into account rights and values should therefore be developed by DPAs. However, this has not been the case so far. Even though the GDPR underlines the importance of safeguarding rights and freedoms of individuals and of societal issues, currently developed DPIA models continue to ignore societal repercussions.[335] Incentives to change current practices could be given by enforcement actions or additional guidelines at the national level.

[332] Ibid.

[333] Ibid 755.

[334] Article 29 Working Party, 'Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679' (n 12); Peter J. Burgess and others, 'Towards a Digital Ethics' (*EDPS Ethics Advisory Group*, 2018) <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf> accessed 1 July 2022.

[335] Mantelero (n 330).

Mantelero developed a rights-based Human Rights, Ethical and Social Impact Assessment (HRESIA) model, which addresses the limitations of current DPIA approaches. It moves the focus from data protection alone by adding, social, ethical and human rights considerations to an impact assessment analysis of data processing activities. It promotes safeguarding rights and values and accountability in relation to IoT and other technology development, in line with GDPR's often mentioned necessity to protect data subjects' fundamental rights and freedoms. HRESIA also underlines the significance of ethical and social values in impact assessments thereby making 'explicit the non-legal values that inform the courts and DPAs in their reasoning when they apply general principles of data protection, interpret general clauses or balance conflicting interests'.[336] Mantelero is conscious of various issues that a HRESIA model might cause. For example, the principle of non-discrimination has been traditionally associated with specific categories such as race, colour, language or religion whereas discrimination through algorithms is founded on vague and not so well-defined conditions. Nevertheless, and whether or not his version of the impact assessment will be adopted by organisations and promoted by regulators, HRESIA has the potential of making an important contribution to explain and implement what other approaches 'leave abstract and disconnected from the ground level', while also abandoning the 'restricted values and principles' of other types of DPIAs.[337] The HRESIA model does certainly seem to be a step in the right direction, towards a better protection of vulnerable people's rights when the latter use data intensive products such as smart devices. The GDPR introduced the 'conceptual novelty of a risk to the rights of the data subjects'.[338] This concept is now at the forefront of data controllers' DPIA obligations and its effects will depend on the manner in which it is interpreted and implemented in practice.

2.2.VI Smart Devices Capable of Keeping the Integrity and Confidentiality of Vulnerable People's Personal Data

Hardware and software solutions (regularly updated) as well as internal organisational measures are necessary to ensure the respect of the integrity and confidentiality principle, which is a prerequisite for lawful processing of personal data (2.2.VI.A). Standards could help

[336] Ibid.

[337] Charles D. Raab, 'Information Privacy, Impact Assessment, and the Place of Ethics' (2020) Computer Law & Security Review 105404, 12.

[338] Van Dijk, Gellert and Rommetveit 303 (n 317).

organisations in meeting the requirements of this principle (but also others to a certain extent) and in ensuring a higher level of protection of vulnerable people's data (2.2.VI.B).

2.2.VI.A Integrity and Confidentiality as a Prerequisite for Lawful Processing and an On-Going Process

How can the integrity and confidentiality principle help in protecting vulnerable people's data when the latter use smart devices? Why is it important in this particular context? From smart devices designed for children that made voice recordings and took pictures (assumed to be private by data subjects) available to the public or effortlessly accessible by third-parties, to hacked smart heating systems that allowed cybercriminals to distort or damage them and burglaries that happened as a result of compromised smart locks, there are many security issues that vulnerable people might have to face if they live within a smart home.[339] For example, in 2015, the company Mattel created an IoT product, the Hello Barbie doll, which has the capacity to listen and talk with children. This toy is equipped with a microphone which records children's voices and transfers them to third-parties for data analysis. The doll was easily hacked by a researcher who gained access to the device's files (including audio recordings) and was able to use the doll's microphone.[340] Similarly, another doll named Cayla was accused by German authorities of spying on smart home members and sending the data it gathered to the United States.[341] Finally, another example is the hacking of Vtech, a company producing digital baby monitors compromising information of more than 5 million customer accounts and children profiles, or the many stories of hackers accessing digital baby monitors and talking to infants through them.[342] These devices endanger vulnerable users and lead to GDPR compliance issues by undermining the security of consumers' personal data.

[339] DCMS, 'Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report' (2018) <https://www.gov.uk/government/publications/secure-by-design-report> accessed 1 July 2022.

[340] Samuel Gibbs, 'Hackers can Hijack Wi-Fi Hello Barbie to Spy on your Children' (*The Guardian*, 26 November 2015) <https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children> accessed 1 July 2022.

[341] Forbrukerradet (Norwegian Consumer Council), '#Toyfail An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys' (December 2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf> accessed 1 July 2022; Bouvet on behalf of the Norwegian Consumer Council, 'Investigation of Privacy and Security Issues with Smart Toys' (2 November 2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf> accessed 1 July 2022.

[342] Deborah Lupton and Ben Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for their Rights' (2017) 19(5) New Media & Society 780.

Security by design requires data controllers to adopt suitable security measures in order to protect against illegal access, data leaks and data breaches.[343] The meaning of 'by design' and what data protection by design signifies more broadly has been explained in part 2.2.IV of this section. Even before the GDPR entered into force, the CJEU had regularly stated that data security is 'an essential component of the protection of individuals with regard to the processing of personal data'.[344] With the establishment of the 'integrity and confidentiality' principle, Art. 5 of the GPDR has raised the act of ensuring data security from a simple requirement to one of the main data protection principles.[345] This means that organisations violating this principle could receive the highest fines provided for in the regulation. Art 5.1 (f) of the GDPR states that 'personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")'. Rec. 39 of the GDPR adds that 'personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing'.

Art. 32 of the GDPR requires the adoption of state-of-the-art security mechanisms. Examples of such measures are pseudonymisation and encryption of personal data or the 'adherence to an approved code of conduct or an approved certification mechanism'.[346] Even though this topic has been widely discussed by experts following the adoption of the GDPR, the specific nature of a state-of-the-art security measure has still not been defined.[347] This is probably partly due to the ever-changing nature of technology and its efficacy. For example, at one time, certain data anonymisation measures have been praised by some and then harshly criticised by others for not being able to ensure data security.[348] The cost of adopting state-of-the-art security mechanisms needs to be proportionate to the significance and likelihood of potential risks.[349] As ENISA affirms, 'the higher the risk, the more rigorous the measures that the controller or

[343] DCMS, 'Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report' (n 339).

[344] Ni Loideain 188 (n 208); European Commission v Republic of Austria, Case C-614/10, [2012] (ECLI:EU:C:2012:631).

[345] Ni Loideain 187 (n 208).

[346] FRA, 'Handbook on European Data Protection Law' (n 256).

[347] Hansen, 'Data Protection by Design and by Default à la European General Data Protection Regulation' (n 287).

[348] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57(6) UCLA Law Review 1701.

[349] FRA, 'Handbook on European Data Protection Law' (n 256)

the processor needs to take (in order to manage the risk)'.[350] In the case of vulnerable people, those risks would be certainly greater (as we have seen in the section on DPIAs, processing vulnerable people's data by smart devices is likely to result in a high risk). Moreover, considering the increasing number of security breaches in the IoT world, there are currently high risks associated with the use of such products. It is also important to remember that security of personal data is not only attained through relevant hardware and software solutions but also internal organisational processes such as the training and education of an organisation's employees about data security rules, or a clear allocation of data processing tasks to selected persons.[351] Indeed, organisational measures and hardware or software solutions influence each other. A recent paper has shown (through semi-structured interviews) how most developers from the software engineering community (aside from certain specific domains) are not encouraged to make data protection their priority and how they are obliged to conform to their organisations' practices of not prioritising privacy.[352] Moreover, they often do not have enough understanding of data protection and how technologies can support privacy through design processes. Internal practices of an organisation have a strong impact on the security solutions adopted in smart products.

If possible, developers of smart devices should implement state-of-the-art solutions already during the design process. However, some authors argue that this could be problematic for IoT devices 'with simplistic functionality or low computational power', which cannot always use intensive processes such as encryption.[353] For example, in the smart health care setting, it has been suggested to use 'lightweight cryptographic algorithms that can be implemented on resource-constrained IoT devices connected via low energy networks' as the low computing power of many smart products makes it difficult to implement complex data security algorithms.[354] Moreover, one data security policy will not be possible or appropriate to implement in all situations also because of a lack of resources of certain organisations (of course, this would not release such a company from the obligation of adopting effective

[350] ENISA, 'Reinforcing Trust and Security in the Area of Electronic Communications and Online Services. Sketching the Notion of 'State-of-the-Art' for SMEs in Security of Personal Data Processing' (28 January 2019) <https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-in-the-area-of-electronic-communications-and-online-services> accessed 1 July 2022.
[351] FRA, 'Handbook on European Data Protection Law' (n 256).
[352] Irit Hadar and others, 'Privacy by Designers: Software Developers' Privacy Mindset' (2018) 23(1) Empirical Software Engineering 259.
[353] Wachter (n 55).
[354] Sherali Zeadally and others, 'Smart Healthcare: Challenges and Potential Solutions Using Internet of Things (IoT) and Big Data Analytics' (2020) 4(2) PSU Research Review 93.

security mechanisms) .[355] Finally, the efficacy of protection measures that have been adopted can rapidly decline because of unpredicted system weaknesses, new kinds of attacks and new security features on the market. As a result, in order to respect the principle of integrity and confidentiality, organisations developing and deploying smart products need to make a long-term commitment to the consumer that they will actively work to discover potential threats and update their products and services accordingly.[356]

Ensuring the security of data is a prerequisite for lawful data processing. Art. 4 (12) of the GDPR states that a data breach is a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. Those processing activities of deleting, disclosing or accessing data are not as such illegal.[357] If the controller is found to have taken relevant security measures and to not have been negligent, the data breach will be considered accidental[358]. If, however, appropriate data protection safeguards are not implemented and a data breach occurs as a result, this would be a clear violation of the integrity and confidentiality principle and it would make the use of any legal basis unlawful. This is evaluated on a case-by-case basis.[359] Implementing the integrity and confidentiality principle is a precondition for GDPR-compliant processing. Over the last few years, it has been proven that hackers were able to use Amazon Alexa and Google Home smart assistants in order to spy on data subjects without their knowledge, or to deceive them into giving sensitive personal information.[360] This has happened several times even though Amazon and Google have deployed countermeasures after each attack. Vulnerable people cannot be expected to understand when an IoT device is behaving in an unusual manner and to spot a data security threat. Those devices should ensure that security measures are sufficiently strong. While a data breach can theoretically always happen, the fact that it does over and over again is a worrying sign. In this case, would authorities consider the data breach as accidental? If countermeasures adopted by Google and Amazon are regularly proven ineffective over relatively short periods of time then the answer should probably gravitate

[355] Rodrigo Roman, Pablo Najera and Javier Lopez, 'Securing the Internet of Things' (2011) 44(9) Computer 51.
[356] Wachter 274 (n 55).
[357] Clifford and Ausloos (n 221).
[358] Ibid.
[359] Ni Loideain (n 208).
[360] Catalin Cimpanu, 'Alexa and Google Home Devices Leveraged to Phish and Eavesdrop on Users, Again' (*ZDNet*, 20 October 2019) <https://www.zdnet.com/article/alexa-and-google-home-devices-leveraged-to-phish-and-eavesdrop-on-users-again/> accessed 1 July 2022.

towards a negative response (especially considering the resources at the disposition of those companies).

Confidentiality of a person's data also implies that a device used by multiple users will only grant access to stored data or start collecting data after one of those users' identity has been established.[361] Asking a user to authenticate himself is a frequent feature of IoT products. However, what about a situation when guests enter a room in which data is recorded through a voice assistant? If this device is not programmed to ask guests for consent, should it be? Is the data controller at fault here? Or is informing those guests the responsibility of the device's owner? It would be difficult to argue for the latter when the owner of the IoT product is a vulnerable person such as a child or a person living with dementia. As a consequence, this thesis argues in favour of companies needing to implement sufficiently secure systems that can somehow identify a new person in the household and prevent their data collection, and that can ensure automatic protection of their data through processes such as encryption.

As this PhD has underlined in the introductory chapter, smart devices often lack basic security mechanisms and the number of security breaches is rising every year. Because smart products will be used more and more often by vulnerable people regardless of whether they are designed specifically for them or for the general population, it is crucial to make them as secure as possible. An example of a group of smart devices often used by vulnerable adults are health gadgets. Those products often send special category data of vulnerable individuals to the cloud and this creates high security risks for data subjects.[362] Unauthorised access to smart health devices could pose a serious threat to a vulnerable person's health in addition to the more obvious and general privacy risk. In a smart home setting, those who care for a vulnerable adult or a child should be trained on how to operate and securely use smart devices (for example, through a tutorial they would need to go through before being able to use the device). A recent report shows that the rapid increase of the number of medical IoT products leads to an immense and vulnerable attack surface that can be targeted by cybercriminals.[363] Organisations developing and deploying unsecure smart devices should be held accountable.

[361] Sandra Wachter, 'Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR' (2017) 34(3) Computer Law & Security Report 436.
[362] Zeadally and others (n 354).
[363] Vectra, 'Spotlight Report on Healthcare' (2019) <https://www.vectra.ai/download/spotlight-report-on-healthcare-2019#form-download> accessed 1 July 2022.

It is possible to argue based on GDPR provisions that if a device is likely to be used by vulnerable persons, organisations need to go even further in terms of ensuring the security of their products as the regulation mandates the controller to take special protection measures in relation to children and other vulnerable individuals (for example, Rec. 75 and 38 but also, in relation to children, Art. 6.1 (f), 8, 12, 40.2 (g) and 57.1 (b) GDPR). Of course, both data of ordinary citizens and vulnerable people require a high level of protection. However, it seems plausible that in case of an infringement procedure, the enforcing authority will look at the security mechanisms adopted by the controller in even more detail if its devices are mostly used by vulnerable members of society (in the spirit of the GDPR that requires special focus on the latter). If organisations continue to develop devices lacking sufficient security features, it is a priority first to ensure adequate protection of the most vulnerable members of society as best as possible while at the same time pushing towards an overall improvement of the security of those products.

Security of data is discussed in other parts of the thesis as well. Devices need to have strong security measures embedded into their design but their security is also strongly linked to the privacy protective technologies and architectures within which they operate. Specific architectures and technologies will be evaluated in Chapter 4.

In the next paragraphs, the present chapter will focus on evaluating why standardisation in the IoT sector is essential and why it could improve the security of personal data if done in the right manner. Standards can help in ensuring safe data processing.[364] Compliance with relevant standards would help organisations in proving that they take the requirement of ensuring the integrity and confidentiality of their data subjects' data seriously.

2.2.VI.B The Importance of Standards for GDPR Compliance in the Field of Domestic IoT

Why are standards relevant to this doctrinal study? In the *James Elliot* case, the CJEU decided that harmonised standards are part of EU law[365]. A harmonised standard is a 'European standard developed by a recognised European Standards Organisation: CEN, CENELEC, or ETSI. It is

[364] FRA, 'Handbook on European Data Protection Law' (n 256).

[365] James Elliott Construction Limited v Irish Asphalt Limited, Case C-613/14, [2016] (ECLI:EU:C:2016:821).

created following a request from the European Commission to one of these organisations. Manufacturers, other economic operators, or conformity assessment bodies can use harmonised standards to demonstrate that products, services, or processes comply with relevant EU legislation'.[366] A standard more broadly can be defined as a 'technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory'.[367] Notwithstanding the fact that standards are usually not legally binding, they are rules that can shape data protection law. They influence how smart devices are made and how the IoT field operates as they have an impact on the actions of both public and private organisations.

Standards can be implemented on a voluntary basis. This is because organisations' compliance with standards is often seen as proof of due diligence and best practice in a specific sector.[368] Organisations are therefore incentivised to comply with standards. As a result of their compliance, they could be considered as more reliable and reputable by all actors.[369] For example, the company called EUSoft (it develops software to manage laboratory testing) advertises on its webpage that it respects the ISO 27001 standards related to security and safety.[370]

Public and private law can also influence the adoption of standards. Standards can be imposed on organisations or they can be implemented as a result of negotiations between businesses.[371] Public law can impose the adoption of standards through legal rules or guidelines. Government officials frequently use standards to create legislation and best practice guides. The European Commission has even published a report explaining how to reference standards in legislation.[372]

[366] European Commission, 'Harmonised Standards' (2019) <https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en> accessed 1 July 2022.

[367] Regulation (EU) 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, [2021] OJ L 316/12.

[368] Niamh Christina Gleeson and Ian Walden, ''It's a Jungle Out There'?: Cloud Computing, Standards and the Law' (2014) 5(2) European Journal of Law and Technology.

[369] Beniamino Di Martino and others, 'Internet of Things Reference Architectures, Security and Interoperability: A Survey' (2018) 1(2) Internet of Things 99.

[370] EUSoft, 'We are ISO 27001 Certified!' (28 March 2019) <https://www.eusoft.co.uk/we-are-iso-27001-certified/> accessed 1 July 2022.

[371] Gleeson and Walden (n 368).

[372] European Commission, 'Methods of Referencing Standards in Legislation with an Emphasis on European Legislation' (2002)

Compliance with standards can be useful in proving that an organisation also complies with laws.[373] Private law often imposes standards as a result of negotiations or enforcement through contractual agreements.[374]

There are various categories of standards. They can be technical, informational and evaluative.[375] Technical standards are defined as giving information on 'a format, protocol, or interface and describe how to make things work in an interoperable manner'.[376] They are usually developed by industry actors and, as a consequence, are more frequently governed by private law. Their impact on consumer behaviour and business practices can be as significant as that of other categories of regulations and laws.[377] The objective of informational standards is to 'set parameters for types of information to be communicated about a product, such as labelling standards'.[378] Finally, the mission of evaluative standards is to 'test and certify the proper use of best-known practices'.[379] Legislators regularly use informational and evaluative standards as an element of their response to policy concerns.[380]

UK and EU organisations mapped standards in the following documents: the Department for Digital, Culture, Media and Sport's (DCMS) 'Code of Practice for Consumer Internet of Things (IoT) Security'[381] and the associated 'Mapping of IoT security recommendations, guidance and standards to the UK's Code of Practice for Consumer IoT Security' (2018)[382]; the 'European Union Agency for Network and Information Security' (ENISA) 'IoT Security Standards Gap Analysis, Mapping of Existing Standards Against Requirements on Security

<https://ec.europa.eu/docsroom/documents/3276/attachments/1/translations/en/renditions/native> accessed 1 July 2022.

[373] Gleeson and Walden (n 368); BSI, 'Standards and Regulation' (2021) <https://www.bsigroup.com/en-GB/standards/Information-about-standards/standards-and-regulation/> accessed 1 July 2022.

[374] Gleeson and Walden (n 368).

[375] Ibid.

[376] Nathaniel Borenstein and James Blake, 'Cloud Computing Standards: Where's the Beef?' (2011) 15(3) Ieee Internet Comput 74, 75.

[377] Gleeson and Walden (n 368).

[378] OECD, 'OECD Policy Roundtable on Standard-Setting' (2010) <http://www.oecd.org/daf/competition/47381304.pdf> accessed 1 July 2022.

[379] Borenstein and Blake 75 (n 376).

[380] Gleeson and Walden (n 368).

[381] DCMS, 'Code of Practice for Consumer IoT Security' (October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf> accessed 1 July 2022.

[382] DCMS, 'Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security' (October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/774438/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf> accessed 1 July 2022.

and Privacy in the Area of IoT' (2018)[383]; the ETSI globally applicable standard for consumer IoT cybersecurity (2019).[384] The latter is the first internationally applicable standard in the field of consumer IoT cybersecurity.

ISO standards are payable international standards and, therefore, not part of the EU legal framework and not accessible to all. Especially smaller organisations might not always see the benefit of investing in a particular standard with the limited funding they have. However, some organisations do use them in their compliance efforts. Examples of ISO privacy-related standards and projects (but not specifically IoT-related) are: the ISO 27701 standard, which is a privacy extension to the ISO 27001 standard on information management systems and the ISO 27002 on security controls (this standard provides guidance in terms of protection of privacy, for example concerning management of personal data)[385]; ISO/IEC 29184 standard on online privacy notices and consent[386]; the ISO project to create a first set of international guidelines with the objective of embedding privacy into the design of products and services, both to facilitate compliance with regulations and to increase consumers' trust in online services.[387]

Despite recent developments and the publication of standards and codes of practice mentioned above, there are still 'significant shortcomings in many products on the market'.[388] Numerous organisations seem to ignore recommendations included in those documents (the recent or insufficient standards' harmonisation may be one of the reasons).[389] A large number of IoT

[383] ENISA, 'IoT Security Standards Gap Analysis' (17 January 2019) <https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis> accessed 1 July 2022.

[384] Sophia Antipolis, 'ETSI Releases First Globally Applicable Standard for Consumer IoT Security ' (*ETSI*, 19 February 2019) <https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security> accessed 1 July 2022; ETSI, 'EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements' (June 2020) <https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf> accessed 1 July 2022.

[385] ISO, 'ISO/IEC 27701:2019 Security Techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management - Requirements and Guidelines' (August 2019) <https://www.iso.org/standard/71670.html> accessed 1 July 2022.

[386] ISO, 'BS ISO/IEC 29184 Information Technology - Online Privacy Notices and Consent' (2018) <https://standardsdevelopment.bsigroup.com/projects/2016-01083> accessed 1 July 2022.

[387] ISO, 'ISO/PC 317 Consumer Protection: Privacy by Design for Consumer Goods and Services ' (2018) <https://www.iso.org/committee/6935430.html> accessed 1 July 2022.

[388] DCMS, 'Consultation on the Government's Regulatory Proposals regarding Consumer Internet of Things (IoT) Security' (n 218).

[389] Jiahong Chen and Lachlan Urquhart, '"They're all about pushing the products and shiny things rather than fundamental security": Mapping socio-technical challenges in securing the smart home' (2022) 31(1) Information & Communications Technology Law 99, 117.

products, such as smart medical devices used by vulnerable people at home, still lack effective security standards.[390] Risks to personal data are omnipresent. For example, the absence of appropriate security features in those medical devices in combination with the possibility to track them through search engines such as Shodan can make vulnerable data subjects an easy target, exposed to all sorts of criminal attacks.[391] The lack of standards' implementation at a large scale can be also due to the potential costs, which organisations want to avoid or just because they do not see any incentive to do so. While some of them will implement security standards out of concern for their customers, many will ignore it without further incentive to change their approach. Even if organisations do not fear GDPR enforcement mechanisms or have not considered them in their processes, certification mechanisms and labelling schemes could push them to change their actions. It is highly probable that consumers will have a preference in favour of products certified through a labelling scheme and this could incentivise organisations to comply with IoT standards.

Certification mechanisms are indeed further evidence of the importance of standards for users and developers of smart products. The objective of certification is to prove compliance with a group of standards. It can be described as 'conformity assessment' which serves 'to evaluate compliance of persons, products and/or processes with a given set of requirements'.[392] To demonstrate compliance with evaluative standards (which prove that certain levels of quality and security have been attained), third party certification is often necessary.[393] Especially in the field of safety and security, an independent certification body should perform the certification. The GDPR states that 'in order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services' (Rec. 100 and Art. 42 GDPR). Art. 43 affirms that 'adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller'. In particular, certification mechanisms and codes of conduct can be used to demonstrate compliance with the principle of integrity and

[390] Zeadally and others 5 (n 354).
[391] Ibid.
[392] ENISA, 'Security Certification Practice in the EU' (21 November 2013) <https://www.enisa.europa.eu/publications/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study> accessed 1 July 2022.
[393] Gleeson and Walden (n 368).

confidentiality as well as data protection by design and by default (Art. 25 and Art. 32 GDPR). The ICO encourages their development.[394] Certification mechanisms can strengthen confidence and trust among those who buy smart home products because they show that a particular device implements specific standards.[395]

Labelling schemes have been recently put forward by industry, certification bodies and the government.[396] Perhaps most importantly – as this could greatly influence the whole IoT sector – the government proposed a labelling scheme for consumer IoT product security.[397] This has been already mentioned in the section on transparency as such a scheme could help consumers in making more informed choices. However, it would have other implications as well by increasing the security of smart devices and facilitating GDPR compliance with the integrity and confidentiality principle as well as data protection by design and default. Customers could also be persuaded by industry certification schemes, such as the Kitemark for IoT devices (the first such certification in this sector), published in May 2018.[398] The British Standards Institution (BSI) considers that this Kitemark is 'one of the most recognised symbols of quality and safety' giving 'true value to consumers, businesses and procurement practices'.[399] Buyers of smart products could consider that if a device is certified through this Kitemark, they do not need to be preoccupied by any safety and security risks. In fact, 'standards and certificates can be a synonym of reliability and assurance to the end user and citizen'[400]. This is another reason why the way standards are being written is crucial for the IoT sector. There is a need of effective standards and the assumptions upon which they are based need to be correct. Otherwise, consumers might blindly trust certifications and jeopardise their own security and safety. How does one standard interact with another? What are the criteria against which the certification is

[394] Information Commissioner's Office, 'ICO Codes of Conduct and Certification Schemes Open for Business' (28 February 2020) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/02/ico-codes-of-conduct-and-certification-schemes-open-for-business/> accessed 1 July 2022.

[395] Irene Kamara, Thordis Sveinsdottir and Simone Wurster, 'Raising Trust in Security Products and Systems through Standardisation and Certification: The Crisp Approach' (ITU Kaleidoscope: Trust in the Information Society (K-2015), Barcelona, December 2015).

[396] Shane D. Johnson and others, 'The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay' (2020) 15(1) PLOS ONE 1.

[397] DCMS, 'Consultation on the Government's Regulatory Proposals regarding Consumer Internet of Things (IoT) Security' (n 218).

[398] BSI, 'BSI Launches Kitemark for Internet of Things Devices' (15 May 2018) <https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/may/bsi-launches-kitemark-for-internet-of-things-devices/> accessed 1 July 2022.

[399] BSI, 'BSI Kitemark for Products' (2019) <https://www.bsigroup.com/en-GB/kitemark/product-testing/> accessed 1 July 2022.

[400] Kamara, Sveinsdottir and Wurster 2 (n 395).

done? What does safe mean in the context of IoT products? These are crucial questions that need well thought out responses. The right standards could help with GDPR compliance, strengthen consumers' rights and help the latter in making more secure choices. In particular, they could be a simple and effective way of communicating to vulnerable persons or their legally authorised representatives that the organisation has implemented appropriate security measures (or at least some of them).

Lawrence Lessig discussed what he called regulation through code, and how the design and architecture of technologies can become regulatory instruments that have the ability to enforce certain laws.[401] Indeed, standards can shape the development of smart devices, influence how people interact with them and how they behave. In the same spirit, Reidenberg declared in 1997 that organisations writing standards, members of 'the technical community, willingly or not, now' have 'become a policy community, and with policy influence comes public responsibility'.[402] Harmonised EU and UK standards form an important part of legal regulation because they can translate and materialise abstract legal principles in specific contexts and, as a consequence, facilitate compliance and enforcement. Organisations developing and deploying smart devices used by vulnerable people should be supported by standards.

In the third chapter of this thesis (the empirical part), during semi-structured interviews, professionals working for organisations developing and deploying smart devices described how they implement standards and certifications, and how they evaluate their current role in facilitating GDPR compliance. This will be developed in the next part of the PhD.

Section 2.3 Conclusion – Lessons Learned from this Chapter's Findings

How has this part of the thesis contributed to respond to this PhD's main research question concerning the workings of data protection law in the context of smart devices used by vulnerable people? Firstly, the most relevant GDPR provisions have been analysed and advice on how to implement them to ensure compliance in this particular context has been provided. Secondly, this chapter proposed future directions towards which legal provisions, guidelines, standards and data controllers' actions should evolve in the data protection IoT field. Thirdly,

[401] Lawrence Lessig, *Code: Version 2.0* (Basic Books 30 December 2006).
[402] Joel R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76(3) Texas Law Review 553, 592.

it established which GDPR principles should be prioritised to increase the protection of vulnerable people's data and facilitate legal compliance.

This chapter has been divided into two parts. In the beginning, it discussed the choice of the most appropriate legal basis by data controllers (the lawfulness principle). The objective of this analysis has been to reflect on the relevant legal grounds and their requirements when a child or a vulnerable adult uses a smart product. Subsequently, pertinent GDPR principles have been critically discussed in order to better understand how they apply to IoT devices gathering vulnerable people's personal data. Without repeating all the findings, this study will now synthesize some of the main arguments of the doctrinal analysis.

While this thesis argues in favour of preventing issues and reducing personal data processing by focussing organisations' attention on the principles of data minimisation, security, data protection by design and by default (DPbDD) and on data protection impact assessments (DPIAs), the appropriate implementation of a relevant legal ground remains crucial in situations in which processing of personal data cannot be avoided and when data subjects have explicitly expressed their wish for their data to be processed. Moreover, no security measure is perfect and risks of data breaches will always exist. Controllers need to make sure they satisfy all GDPR requirements before the processing starts and that data subjects make informed decisions. The choice of a legal basis will depend on the context and should be done on a case-by-case basis. In certain situations, consent could be appropriate while in others it will be legitimate interests, performance of a contract or vital interests (these are the relevant legal bases for this study under Art. 6 of the GDPR). Special category data processing would require the organisation to choose an additional distinct legal ground under Art. 9 of the GDPR. Regardless of the legal basis's choice, the data controller is required to adopt special data protection measures in relation to vulnerable individuals and to adapt its actions to the latter's needs in order to safeguard their fundamental rights and freedoms.

This PhD has evaluated consent requirements by giving examples of situations involving vulnerable people using smart products and how organisations should adapt to them. Most importantly, what this thesis considers is that for smart devices used by everyone (for example, voice assistants), measures supporting vulnerable individuals (such as those proposed by the ICO in its Age Appropriate Design code of practice) should be automatically adopted for all data subjects. The UK data protection authority has suggested, among others, to present privacy notices in clear, plain and age-appropriate language. Using simple terms and clear concepts should be standardised practice for all privacy policies as most people cannot comprehend the technical and convoluted language that they usually adopt. This does not mean that special measures applicable only to a specific group of vulnerable individuals should not exist. For example, smart devices targeting people living with dementia might have to adapt their consent gathering mechanisms to the particular needs of this group of people.

There are three other legal bases that organisations developing and deploying smart devices could potentially use to process vulnerable people's data. They have all been analysed in detail in this chapter by giving examples of smart products and concrete situations. In certain circumstances, the performance of a contract legal basis might be the most relevant choice. To be able to use this legal ground, processing must be necessary for the execution of a contract. Fewer conditions need to be satisfied than in the context of consent so this basis is easier to implement for an organisation. However, the necessity condition implies that the purpose of data processing is genuinely understood from the perspective of an average data subject. Organisations would need to make sure that this is the case when vulnerable people are their consumers. Relying on the performance of a contract to process special category data by an IoT device could only be lawful in the context of an agreement with a health professional for purposes of preventive or occupational medicine (Art. 9.2 (h) GDPR). Another legal ground that could be used is legitimate interests. In this case (according to current guidelines and the GDPR), extra care needs to be taken to safeguard children's and vulnerable adults' rights and freedoms from risks they might not fully comprehend and from consequences they may not predict. In addition to a more compelling interest when processing vulnerable people's data gathered through smart devices, appropriate safeguards would need to be implemented (such as age restrictions). A vulnerable data subject must reasonably expect that their data will be gathered for legitimate interests to be lawful. Moreover, a balancing exercise of a data controller's interests against the fundamental rights and freedoms of its data subjects would need to be performed. Enforcement difficulties and data controllers' lack of knowledge on how to perform balancing exercises suggests that in-depth balancing tests could be the exception rather than the rule. No corresponding legal ground to legitimate interests exists to process special category data through smart products in smart homes. Finally, the last legal basis that has been discussed in this chapter is vital interests. Data controllers will only be able to use it in matters of life and death, when the data subject is incapable of giving consent. Most organisations developing and deploying IoT devices will not be able to rely on this basis but for those working in the health sector, it could be relevant if their devices are capable of saving lives.

In addition to lawfulness, in the same GDPR provision (Art. 5.1 (a)), two other principles are mentioned – transparency and fairness. They are essential to ensure an effective protection of vulnerable people's rights. Transparency requires information to be concise, intelligible and easily accessible. Issues such as the unacceptable manner of updating and communicating privacy policies in the IoT sector or the recurring lack of user interfaces on smart products have been discussed. Guidelines (WP29's and ICO's), CJEU cases and GDPR provisions confirm the necessity to adopt special measures to ensure that information is provided transparently to vulnerable people in all communications with them. Compliance with the transparency principle can also be increased through other GDPR mechanisms, for example, by publishing data protection impact assessments, adhering to codes of conduct and labelling schemes. Just like with consent requirements, this thesis argues in favour of always assuming that a vulnerable person might use a smart device and of adapting communication mechanisms by default to the latter's needs. Indeed, any smart device could be used by a vulnerable person and anyone could become vulnerable over time. Other citizens would also benefit from such special data protection measures as they would increase transparency and their data protection in general.

In terms of the fairness principle, current legal literature seems to give this tenet two main meanings. Firstly, fairness requires transparency but is distinct from the latter. A smart device might be transparently communicating information to ordinary citizens but if it ignores the needs of the minority of people with mental disabilities that also use it, this would not be 'fair transparency'. Secondly, fairness requires data controllers to perform balancing exercises, often implicitly required by the GDPR and which are context dependent. Currently, fairness is not a well understood concept. There is potential for this principle to support human dignity in technologies of the future, such as smart products. The European Data Protection Supervisor has called for an urgent reflection on ethics and data protection, partly by underlining the importance of discussing how the fairness principle should be perceived in this context.[403]

[403] EDPS, 'Opinion 4/2015 Towards a New Digital Ethics' (n 257).

As it has been mentioned above, this thesis argues that focussing on the lawful processing of personal data should not be an organisation's first priority. When a data controller does decide to gather vulnerable people's data, this is precisely where problems might appear. If consent is taken as an example, satisfying its conditions and adopting special measures to protect vulnerable people's personal data requires much effort and the more data is collected, the more issues can arise (for data controllers in terms of compliance and for data subjects in terms of their data protection rights). Secondly, consent has been criticised by some researchers as not giving real control over how data is processed and as being gathered in a situation of power imbalance, this argument being even more relevant in the context of vulnerable people. It is widely known for instance that people rarely read privacy notices even if they are written in clear terms. This power imbalance also exists for other legal bases, for example, when an organisation uses legitimate interests and weights its own interests against those of data subjects. In order to protect children's and vulnerable adults' fundamental freedoms and rights as well as facilitate compliance for data controllers, this PhD underlines the importance of the following GDPR mechanisms: data minimisation, DPbDD, DPIAs and the integrity and confidentiality principle. They should be promoted, implemented and enhanced as they are capable of preventing problems and giving more power to vulnerable individuals. Only after this has been done as best as possible, an organisation should evaluate what legal basis to use if processing vulnerable people's personal data is still needed.

Firstly, concerning the principle of data minimisation, its objective is to ensure that personal data processing is adequate, relevant and restricted to the minimum necessary. Personal data needs to be processed only if the purpose of processing cannot be achieved by other means. This is in stark contrast to the 'data maximalism' associated with the huge amounts of data collected by IoT products, stored and usually analysed in the cloud. Regulators have underlined the importance of implementing the principles of data minimisation even more strictly when smart devices are used by children (or vulnerable adults). Minimising their data collection will minimise the many risks associated with data processing and with implementing appropriate legal bases, those risks being substantially increased for vulnerable individuals.

Secondly, the implementation of the data protection by design and by default principle has become a mandatory requirement in the GDPR. Just like data minimisation, the by design approach is essential for vulnerable people who have less capacities to protect themselves against data breaches or to comprehend what kind of data is being processed and what this involves. This is linked to the data protection by default principle and the necessity to limit data processing to what is necessary for simply using an IoT product. Vulnerable people might not be capable of exercising effective active control over the processing of their data so turning non-essential processing off by default is essential. Unfortunately, this is not the reality at the moment and many IoT devices continue to transfer personal data to third-parties without even informing the data subject about these activities.

Thirdly, DPIAs are an important element of a data controller's obligations that contribute to meeting the requirements of various data protection principles such as the accountability principle or data protection by design and by default. Whenever there is potential for a high risk, a DPIA will need to be carried out. Processing vulnerable people's personal data gathered through smart devices will always require an impact assessment as this represents a situation that might result in high risks according to ICO's and WP29's criteria. DPIAs became mandatory with the entry into force of the GDPR. They can be described as 'meta-regulation', which means that while organisations are free to choose their own DPIA self-management processes, they are also externally accountable for the latter. The effectiveness of meta-regulation will be dependent on the capacity of data protection authorities to evaluate organisations' risk reduction plans (which seems to be an issue at the moment). Stakeholder involvement in DPIAs is suggested in the GDPR but unfortunately not mandatory. Including relevant vulnerable groups of people and their legal guardians into the impact assessment process could improve the understanding of their data protection needs and help in safeguarding their rights and freedoms. A values-oriented impact assessment model, such as the one proposed by Professor Mantelero, is in line with GDPR's frequently mentioned importance of protecting data subjects' fundamental rights and freedoms.[404] This thesis considers that DPIAs should not only evaluate risks to data protection rights (currently the prevalent approach) but also consider social, ethical and human rights aspects of data processing. These will differ depending on the application domain (for example, health sector versus home environment) and the person involved (there are fundamental rights and freedoms that, for example, only children possess).

[404] Mantelero (n 330).

Finally, security is of course of paramount importance in the IoT field considering the rising number of breaches and malicious actors. Those breaches can have a stronger negative impact on children or vulnerable adults. For this reason, when smart devices process vulnerable people's data, security mechanisms should be state-of-the-art, in conformity with the requirement to adopt measures proportionate to the importance and likelihood of potential risks. IoT devices pose their own particular problems, such as their usually low computation power preventing the adoption of intensive data protection processes such as encryption. However, organisations need to find solutions as the absence of appropriate security measures would violate the integrity and confidentiality principle, which would in turn render any data processing unlawful (even where it is justified with a legal basis). Standards can improve the security of devices and inform vulnerable people about the level of data protection that they are offering. While most IoT devices continue to ignore the implementation of appropriate standards, harmonisation of the latter and the appearance of certification mechanisms such as the BSI IoT Kitemark or the UK government's labelling scheme for consumer IoT product security could hopefully push data controllers to change their behaviour. The implementation of relevant standards could turn into a competitive advantage as consumers will probably prefer products, which have been officially certified as being secure.

In the next third chapter, this thesis will focus on semi-structured interviews, which have been conducted to analyse how topics that have been discussed in the doctrinal study are viewed by professionals dealing with data protection issues on an everyday basis. Subsequently, the last fourth chapter of this PhD will build on this analysis to evaluate how to improve compliance with GDPR principles through edge computing and privacy enhancing technologies.

Chapter 3: Expert Perspectives on GDPR Compliance When Vulnerable People Use Smart Products

This chapter analyses experiences, opinions and perceptions of experts on data protection law compliance when vulnerable people use smart products through interviews with 21 professionals. Firstly, the epistemological assumptions, methods, methodology and data analysis processes linked to this study are explained (Section 3.1). In the second section, results of the theme generation process are briefly described (Section 3.2). Subsequently, an in-depth analysis of the interviews is conducted by discussing challenges and opportunities linked to a vulnerability-aware approach to GDPR compliance (Section 3.3), legal challenges encountered by professionals (Section 3.4) and the need of a privacy-preserving holistic technological model to better overcome the latter (Section 3.5). Finally, the sixth section offers a more condensed discussion of the findings of this chapter grouping them into three main categories: challenges linked to the notion of vulnerability; analysing professionals' approach to GDPR implementation when vulnerable people use smart devices; technological barriers and solutions to the legal conundrum (Section 3.6).

Section 3.1 The Nature, Process and Reasons for this Empirical Study

In this section, this thesis introduces the methodological aspects of gathering information through semi-structured interviews conducted with UK and international professionals in the field of data protection law and technology design, with a focus on the smart home context. While the doctrinal efforts in this thesis contributed to the knowledge of how the law should be interpreted and, where necessary, amended, empirical evidence was needed to fill the gap of how the law is understood in practice, in terms of how to comply with it and what the rationales are. In this regard, an interdisciplinary approach has been chosen. It serves both to verify the validity of some of the legal findings and to uncover potentially overlooked theoretical and technological debates explored in the next chapter. It seemed important to interview both technologists and lawyers as the disciplines they represent play a crucial role in this legal and computer science-related thesis. Those discussions gave various insights and perspectives into how the two communities view intricate practical data protection challenges. The main purpose of this research was to better understand how professionals perceive data protection compliance when vulnerable people use smart products. How does GDPR compliance work in practice in this specific context? How do professionals consider data protection-related issues?

Since this study mainly addresses data protection compliance from the perspective of organisations developing and deploying smart devices, the empirical part investigates the understanding and perceptions of legal practitioners and computer scientists working for or advising those organisations. The views of other stakeholders, such as end-users (including vulnerable data subjects, their carers or medical professionals), though important to inform the wider socio-technical picture and specific areas of data protection law, would go beyond the scope of this thesis. Taking into account the general importance of end users' involvement in legal and technological policy making as well as the fact they might not entirely comprehend the legal framework and the various considerations involved, future studies should evaluate how, to what degree and in what areas their expectations and their role should be reflected in data protection provisions and practices.

Concerning reflexivity in this empirical study, that is the question of 'how knowledge is generated and, further, how relations of power influence the processes of knowledge generation', this PhD will now explain its epistemological assumptions, methods, methodology and data analysis processes.[405] In this chapter, the qualitative interpretive epistemological approach was adopted. According to Walsham, interpretive methods of conducting studies consider that our understanding of reality, 'including the domain of human action, is a social construction by human actors' and that 'our theories concerning reality are ways of making sense of the world', shared meaning being 'a form of intersubjectivity rather than objectivity'.[406] Interpretive research was used to analyse how technologists and lawyers subjectively perceive GDPR compliance issues when vulnerable people use smart products. More precisely, this study adopted an interpretative phenomenological approach, which 'does not take account of experience entirely at "face value"' but seeks to comprehend and reflect on the meaning of those accounts in a wider context.[407] The goal of this epistemological stance was to present a more critical commentary of the interviewees' activities and viewpoints.

[405] Heather D'Cruz, Philip Gillingham and Sebastian Melendez, 'Reflexivity, its Meanings and Relevance for Social Work: A Critical Review of the Literature' (2005) 37(1) Brit J Soc Work 73, 77.

[406] Geoff Walsham, 'Doing Interpretive Research' (2006) 15(4) European Journal of Information Systems 320, 320.

[407] Carla Willig, *Introducing Qualitative Research in Psychology* (2 edn, McGraw-Hill Education 2008) 17.

Thematic analysis (TA) was used to evaluate the data. TA can be viewed more as a method rather than a methodology (the latter being a 'theoretically informed, and confined, framework for research'), which does not mean that it is 'atheoretical' but that it can be used within several theoretical frameworks.[408] It should be noted that TA does not refer to one particular analytical tool but to what has been categorised by Braun and Clarke as coding reliability TA (characterised by early theme development, a structured codebook, involvement of multiple coders, informed by positivist paradigms or values), codebook TA (codebook used for coding, pragmatic purposes such as finding specific information, certain themes being developed early as topic summaries, placed somewhere in-between reflexive and coding reliability TA approaches) and reflexive TA.[409] The reflexive TA approach (developed for qualitative paradigms) has been adopted in this study. It can be defined as 'analysis, which can be more inductive or more theoretical/deductive', 'a situated interpretative reflexive process', coding being 'open and organic, with no use of any coding framework' and themes being 'the final "outcome" of data coding and iterative theme development'.[410] In the context of this chapter, the analysis followed an inductive process (based on the collected data). Both semantic and latent themes were developed, the latter going further than the semantic content of the transcripts, evaluating the 'underlying ideas, assumptions, and conceptualizations' which are 'theorized as shaping or informing the semantic content of the data' (capturing its implicit meaning).[411] As a result, the analysis that this PhD strived to produce was not just descriptive but required interpretative work during theme development. After a verbatim transcription of the interviews, Nvivo was used to support the coding process, coding being 'an analytic unit or tool, used by researcher to develop (initial) themes'.[412] Themes are, in contrast to codes 'like multi-faceted crystals – they capture multiple observations or facets'.[413] They are often developed from several codes, although rich and multifaceted codes can sometimes be elevated into the theme category[414]. Most importantly, 'themes are patterns of shared meaning, united by

[408] Victoria Clarke and Virginia Braun, 'Thematic Analysis' (2017) 12(3) The Journal of Positive Psychology 297, 297.

[409] Virginia Braun and Victoria Clarke, 'One Size Fits All? What Counts as Quality Practice in (Reflexive) Thematic Analysis?' (2021) 18(3) Qualitative Research in Psychology 328, 333; Virginia Braun and Victoria Clarke, 'Conceptual and Design Thinking for Thematic Analysis ' (2021) 9(1) Qualitative Psychology 3 ,6-8.

[410] Braun and Clarke, 'One Size Fits All? What Counts as Quality Practice in (Reflexive) Thematic Analysis?' 333 (n 409).

[411] Virginia Braun and Victoria Clarke, 'Using Thematic Analysis in Psychology' (2016) 3(2) Qualitative Research in Psychology 77, 84.

[412] Braun and Clarke, 'One Size Fits All? What Counts as Quality Practice in (Reflexive) Thematic Analysis?' 340 (n 409).

[413] Ibid.

[414] Ibid.

a central concept or idea' that can gather together data, which could at first appear quite heterogeneous.[415] To code and generate themes, the following Braun and Clarke's process was followed: '1) data familiarisation and writing familiarisation notes; 2) systematic data coding; 3) generating initial themes from coded and collated data; 4) developing and reviewing themes; 5) refining, defining and naming themes; and 6) writing the report'.[416]

Preference was given to interviews instead of surveys, in spite of the unavoidable reduced number of participants, as interviews are 'a key way of accessing the interpretations of informants in the field' and they allowed, in combination with the above-mentioned reflexive TA, for a deep investigation of technologists' and lawyers' insights into how data protection law works in practice.[417] Survey questions would not have allowed such an in-depth inquiry as there would not be any direct contact with participants. For the same reason, the choice was made to use semi-structured interviews instead of fully-structured ones. The absence of constraints linked to a rigid set of questions established in advance permitted a more extensive exploration of interesting responses given by the participants. Interviews were chosen instead of direct observation as 'privacy issues are usually not dealt with on a daily basis in most domains, and access to direct observations by researchers from outside the companies is highly restricted'.[418] In addition, the simple presence in the offices of professionals would not have provided expansive insights in terms of their thoughts and perceptions of technical data protection compliance issues.[419]

The interview questions were centred around data protection principles analysed in this thesis, that is the various legal bases, the transparency principle, fairness, data minimisation, data protection by design and by default, data protection impact assessments, standards and certification schemes as well as the privacy-as-confidentiality versus privacy-as-control and edge computing versus cloud computing debates, reflecting many subjects that were discussed in the doctrinal (Chapter 2) and theoretical (Chapter 4) parts of this PhD. Although questions were prepared in advance, freedom was given to interviewees to speak unreservedly, some topics being more expanded upon by technologists than lawyers and vice versa. Their common core was the topic of data protection law compliance when vulnerable people use smart

[415] Ibid 341.
[416] Ibid 331.
[417] Walsham 323 (n 406).
[418] Hadar and others 266 (n 352).
[419] Ibid 267.

products. Questions were refined and evolved during the data collection process to collect richer data, in line with the reflexive thematic analysis process.[420] Sometimes, the interview reflected Socratic dialogue, in which 'the interviewer confronts and also contributes with his or her conceptions' of the interview topic[421]. However, the extent of these interventions was controlled in order to preserve the nature of an interview. Moreover, answers were provided by experts in the field and, as a result, the influence of my own values and interests was limited.

As stated by Myers and Newman, 'situating the researcher as actor' is crucial before the start of the interview process.[422] Elites are accustomed to answering questions and stating their opinions, and an interviewer with certain technical knowledge regarding the subject of the interview can become an engaging conversation partner.[423] It is argued that the interviewer should be informed about the topic of discussion, understand the technical language and learn biographical and social details concerning the interviewee. Indeed, 'an interviewer demonstrating that he or she has a sound knowledge of the interview topic will gain respect and be able to achieve an extent of symmetry in the interview relationship'.[424] In addition to building trust by presenting the background and expertise of the interviewer before interviews began, social dissonance (that is anything that could make the participant feel uneasy) was also reduced, among others, by answering any additional questions related to the content of the consent form, privacy notice and information sheet as well as, similarly to Hadar and others, by 'mirroring the verbal posture and the vocabulary of the participant, and allowing for flexibility in the interview to follow directions the participant found interesting'.[425]

Experts with different professional experiences were chosen to better comprehend, through varied viewpoints, how data protection law compliance works in practice in the context of smart devices used by vulnerable people. Precedence was given to professionals working for companies and law firms to reflect the focus of this chapter on the practical aspects of data protection law compliance. However, several academics were interviewed as well, almost all of them having also participated in university or industry projects related to smart devices and

[420] Braun and Clarke, 'Conceptual and Design Thinking for Thematic Analysis' 12 (n 409).
[421] Svend Brinkmann and Steinar Kvale, *Doing Interviews* (Uwe Flick ed, 2 edn, SAGE 2018) 77.
[422] Michael D. Myers and Michael Newman, 'The Qualitative Interview in IS Research: Examining the Craft' (2007) 17(1) Information and Organization 2, 16.
[423] Brinkmann and Kvale 77 (n 421).
[424] Ibid.
[425] Hadar and others 266 (n 352); Myers and Newman 16 (n 422).

smart homes (more information is provided below on the professional experience of the interviewees). While most professionals worked in the EU and the UK, five interviewees were located outside of Europe. However, they had experience with the GDPR and their work was impacted by its provisions.

As stated by Braun and Clarke, data saturation is not always a helpful and relevant concept for every category of TA research.[426] Indeed, it is not 'philosophically and methodologically consistent with reflexive TA'.[427] In the context of reflexive TA, it is problematic to assert that no new insights can be obtained by collecting new data (even if participants were responding similarly to several questions). This study does not ignore the significance of recurring themes but acknowledges the importance of the quality of a theme and of its relevance to the research question[428]. Saturation ceases to make sense if the analytical process is conceived as developing insights through engagement with the collected data, as there is always room for new readings and interpretations. This study had a specific aim (analysing how data protection law works in practice in the context of vulnerable people using smart products) and specific inclusion criteria (technologists and lawyers). By gathering a diverse and rich data set (this has been subjectively assessed during the data collection process), 'meaning-richness' was considered as achieved, the 'key to the validity of the (size of the) data set'.[429] Indeed, the more in-depth information the collected data contains, the fewer interviewees are required (this is an alternative to saturation in terms of reflecting on justifications regarding the number of required participants within reflexive TA). While the 21 interviews did offer similar insights on various topics from a diverse range of professionals, it was the perceived 'information power' of this data set that resulted in the decision to end the data collection process.[430]

Interviewees were recruited in various ways. Firstly, when this was still possible (before Covid-19), some contacts were established in person at conferences and events. Secondly, direct emails, university and professional networks (LinkedIn and Twitter) as well as websites of

[426] Virginia Braun and Victoria Clarke, 'To Saturate or not to Saturate? Questioning Data Saturation as a Useful Concept for Thematic Analysis and Sample-Size Rationales' (2021) 13(2) Qualitative Research in Sport, Exercise and Health 201, 206.
[427] Braun and Clarke, 'Conceptual and Design Thinking for Thematic Analysis ' 15 (n 409).
[428] Braun and Clarke, 'To Saturate or not to Saturate? Questioning Data Saturation as a Useful Concept for Thematic Analysis and Sample-Size Rationales' 207 (n 426).
[429] Braun and Clarke, 'Conceptual and Design Thinking for Thematic Analysis' 17 (n 409).
[430] Braun and Clarke, 'To Saturate or not to Saturate? Questioning Data Saturation as a Useful Concept for Thematic Analysis and Sample-Size Rationales' 12 (n 426).

relevant organisations helped in identifying and contacting interviewees. There was also the snowball effect of professionals who, after being interviewed, suggested other potential interviewees. Receiving positive responses to interview requests was difficult and the organisation of interviews took a long time. This is probably due to the Covid-19 disruption of work life, to the fact that these were often senior experts with little free time and that some organisations were reticent to share their views (even if it was always mentioned that their responses will be anonymised). It was especially difficult to find interviewees from well-known technological companies. This limited the number of persons who were interviewed. However, as the search for interviewees started early in the PhD journey, this gave enough time to find a diverse interview sample, both small and big companies being represented as well as lawyers and academics, and to engage in interesting conversations fitting the objective and goals of the analysis.

On average, the duration of an interview was 35 minutes (based on the 20 audio-recorded discussions). One person was interviewed in person and nineteen interviews were conducted remotely (Skype or Microsoft Teams). In addition, the 21st interview was not recorded as the interviewee explicitly requested to answer questions in writing. Of course, this specific interview differed as there was no possibility to conduct an in-depth investigation using the semi-structured process. Nonetheless, this one exception has been allowed and the interviewee provided answers based on a similar set of questions as the other interviewees. Consent forms, privacy notices and information sheets were provided to all interviewees before the interviews. This empirical study was formally approved by the University of Nottingham Computer Science Research Ethics Committee.

In terms of data analysis, fictitious pseudonyms were given to all interviewees to preserve their anonymity. To inform the reader about their background, their field of work and years of professional experience have been provided.

Lawyers and DPOs

	Current job/place of work	Years of professional experience	Field of work

Aland	CEO, founder of UK company with 20 employees (part of a larger organisation with around 4000 employees) and Senior Information Regulation Officer	7 years	Smart home devices, digital care for vulnerable and older individuals
Damon	UK Solicitor, Associate at law firm	10 years	Data protection, GDPR, commercial contracts
Neda	Professor of law at university located in the EU, Advisor on children's rights	13 years	Data protection, law, smart technologies and children's rights
Maxwell	Professor of law at UK university and member of a European Commission expert group	8 years	Intellectual property, consumer protection and data protection law
Avena	Data Protection Officer (DPO) at UK charity (over 250 employees)	10 years	Data protection within an organisation supporting vulnerable adults and children (including through smart products)
Farra	UK Solicitor with experience in both public and private sectors	16 years	Data protection and privacy
Joline	Senior Research Analyst (lawyer) at leading UK research, consultancy and	13 years	Law, technology, ethics and society, data protection

	technology development company		
Maeve	Senior Research Analyst (interdisciplinary with a legal background) at leading UK research, consultancy and technology development company	12 years	Privacy, ethical impact assessments of digital technologies, raising awareness about GDPR for professionals and organisations
Kismet	Researcher at university located in the EU	4 years	Human rights law, privacy, data protection, law and technology, children's rights
Lari	Senior Research Fellow at university located in Australia	30 years	Internet of things, privacy, communications law
Edmond	Research Associate at UK university	11 years	Data-driven technologies, datafication and social justice

Designers and technologists

	Current job/place of work	Years of professional experience	Field of work
Laine	Researcher at UK university	8 years	Computer science, human computer interaction, personal

			data, technology design
Finlay	Research Associate at UK university	10 years	Development of ICT technologies, human computer interaction, data-driven processes, smart technologies
Beth	Senior Vice President of large US company (previously worked at one of the largest smart home tech companies with operations in the EU)	23 years	Managing smart home-related advertising, sales, product development, engineering, marketing, legal, finance and operations
Edward	Research Fellow at UK university	8 years	Technology design
Lee	Research Fellow at UK university	27 years	Technology design
Sophia	Founder of a charity organisation, of a start-up and Head of Developer Relations in large international technology company	23 years	Vulnerable people, smart devices, technology development, developer relations
Hazen	Founder of UK SME	17 years	Artificial intelligence, smart devices, technology development
Charlotte	Researcher at US university, Educator on IoT	24 years	Data analytics, product

			development, internet of things
Emily	Industry Analyst and Founder of US company, Member and Analyst at EU company	20 years	Internet of things, new technologies, artificial intelligence, vulnerable groups
Brennan	Chief Technology Officer (CTO) and Founder of UK company (around 10 employees)	23 years	Smart health devices

Section 3.2 Themes Generated through the Analysis of Interviews

After reading the transcribed notes several times as well as coding and re-coding the data, a multitude of themes were generated, developed and refined, finally grouped into seven major categories. All discussions with interviewees organised within the latter responded to at least one of the two research questions of this chapter (also mentioned in the beginning of Section 1), namely: how does GDPR compliance work in practice when vulnerable people use smart products? How do professionals perceive data protection-related issues in this context? By responding to those research questions, this PhD strived to analyse the attitudes of experts to GDPR compliance and evaluate whether interviewees' responses confirmed (or not) legal findings from the second chapter's doctrinal study as well as whether there are any gaps or important topics, which could be addressed in the more theoretical and technology-focussed Chapter 4.

The first major theme entitled lawfulness, transparency and fairness was subdivided into six categories: consent (its advantages and disadvantages for companies and vulnerable people), legitimate interests (as a preferred option for companies to consent and potentially beneficial for vulnerable individuals), performance of a contract (as the recommended option for companies), vital interests (for emerging processing only), transparency and fairness as a useful but vague concept. The second theme focussed on data minimisation and four subthemes were generated, namely: tension with device usefulness, facilitating data protection compliance for IoT organisations and protecting vulnerable people, various degrees of companies' compliance and risks of data overcollection. The third theme analysed DPIAs as multifaceted instruments of evaluating risks. Within the DPbDD fourth theme, five subthemes were developed: experts' knowledge on this topic, the interdisciplinary nature of DPbDD, the objectivity of data protection by default measures, the importance of DPbDD for vulnerable people and companies as well as DPOs as CTOs (technologists working on legal issues). The fifth theme discussed security and confidentiality. It was divided into four subcategories: defining personal data as always potentially personal, the impossible perfection of security measures, experts on confidentiality and control as well as certifications and standards (as compliance tools and uncertainties surrounding them). The sixth theme was named vulnerability-aware approach and analysed the challenges (in terms of defining and considering vulnerable adults and children), solutions (awareness, enforcement and guidance) and the value of this approach. Finally, the last theme presented the need of a new holistic technological model to improve GDPR compliance and three subthemes were generated: issues with the technical identification of vulnerable individuals, design for data co-management and edge architectures as potential solutions.

The themes and sub-themes mentioned above were all used in the analysis but also further regrouped during the last stage of reflexive TA (report writing) into three main sections: a vulnerability-aware approach (Section 3.3), legal GDPR compliance challenges for companies and professionals (Section 3.4), and the need of a privacy-preserving holistic technological model (Section 3.5). Indeed, during the writing process and further in-depth evaluation of the content of discussions with interviewees, this three-fold narrative was developed and certain subthemes needed to be reorganised as they better fitted different parts of the chapter than initially planned during previous stages of reflexive TA. Finally, not all sections and sub-sections are of equal length as only discussions relevant to the research questions were retained during report writing. The subsequent sections present the final result of this PhD's empirical study analytical process.

Section 3.3 Vulnerability-Aware Approach

This part of the empirical chapter does not only present interviewees' opinions and experiences but also critically analyses them. According to this thesis, a vulnerability-aware approach requires considering all data as potentially personal (3.3.I). Several experts underlined the difficulty in defining who is exactly a vulnerable adult and in including them in data protection-related processes (3.3.II). They discussed the need for more education, awareness, guidelines and enforcement in the context of vulnerable persons using smart products (3.3.III). A vulnerability-aware approach would be beneficial not only for vulnerable individuals and to ensure GDPR compliance but also for the general population (3.3.IV).

3.3.I All Data Could be Personal

As discussed in Chapter 1, the distinction between personal and non-personal data is becoming increasingly blurred. This thesis argues in favour of treating data as always potentially personal, especially when considering vulnerable people, the sensitive information their data may contain and the fact that they may be less aware of the risks involved. People could be targeted with their metadata. It is not only personal data that should be protected as any data could lead to or become personal with technological developments and elaborate inferences.[431] This topic was brought up organically by interviewees, pointing to the importance of reflecting on what companies consider as personal data in general, as this will lead them to attribute higher or lower protection levels depending on their interpretation of what this notion entails. Further official guidance on this topic may, therefore, be required to dispel any doubts, in particular in light of the divergent explanations of this concept by professionals.

Responses from interviewees are largely in line with the legal analysis in Chapter 1 that any data could be personal. For example, for Lari (Senior Research Fellow), definitions of personal data tend to be increasingly pointless as 'it's easy enough to anonymise data and use identifiers for people rather than their personal information and you can still target them'. Hazen (Founder of UK SME) stated that once data leaves the smart home, potential users for that data cannot be completely defined at that point in time. More inferences could be made and uses for that data discovered later by companies. However, not all practitioners embraced this approach. For example, Aland (CEO and Senior Information Regulation Officer) stated that:

[431] Purtova (n 6).

> The things that are available on a non-identifiable basis are sensor information readings, things like when a door has been opened or closed, when somebody's made a kettle, that's very low risk, you know. If all of that data was unencrypted and released as de-identifiable data, it's not going to be very useful to anybody. Even things like blood pressure and heart rate might be valuable, but if you haven't got any of the identifiable data behind it, it's not particularly useful for a hacker that wants to get it for financial gain.

3.3.II Challenges in Considering and Defining Vulnerability

Professionals rarely grasp and apply the notion of vulnerable adults within their work processes, especially when products are aimed at the general population. According to several professionals (both solicitors and experts working within IoT companies), organisations do not take vulnerable adults into consideration unless the device is specifically developed for them (according to an interviewee, one reason being that there are mainly references to children in the GDPR and not to other vulnerable individuals). Moreover, Beth (Senior Vice President who worked at some of the biggest IoT companies) stated that even children are often not considered, which further reduces the chances of any consideration of vulnerable adults within companies developing products used by everyone. However, this latter approach is due to premeditated decisions of IoT companies rather than lack of clarity in the GDPR. In conclusion, these issues point both to a lack of guidance and enforcement of GDPR provisions, which were also mentioned by interviewees and will be discussed subsequently in this section.

Apart from inherently vulnerable adults for whom special data protection measures should be always adopted, a major problem in terms of GDPR compliance is the elusive nature of vulnerability and what it means in other contexts. Interviewees underlined the need to work towards a comprehensive UK and EU-wide definition. Most of them stated that vulnerability is context-specific and that there are difficulties in finding an acceptable international definition (one person noted the higher 'popularity' of this term in the UK and the even more pronounced lack of a clear definition in other countries). Some interviewees suggested solutions. For Farra (UK Solicitor), people should not be defined by age but rather based on their 'cognitive ability'. She stated that some sort of 'layered level' of vulnerability could be established based on a set of criteria and that the fairness concept might play a role there. This aligns with this PhD's proposal (in Chapter 1) to consider Luna's theory of layered vulnerability (also reflecting

GDPR's risk-based approach)[432]. Vulnerability is certainly a very context specific notion, and while this thesis has explained its approach of looking at this concept from the perspective of people whose vulnerability layers are always and constantly present, a broader discussion and conclusions are needed in relation to how to approach the notion vulnerability in general in practice so that it can have tangible effects on data protection processes of IoT (and other) companies. The results of those discussions should be published by authorities such as DPAs so that they are actually followed by organisations developing smart products.

3.3.III Education, Guidance and Enforcement as Solutions

Education and awareness is needed in relation to data protection law, both in relation to the public and experts. This has not been discussed in this thesis before but has been presented as crucial by both researchers and professionals. For example, Maeve (Senior Analyst) contended that one reason of bias in the development of digital technologies is that even if their intentions are good, professionals often 'work and act in their own bubbles' without thinking about vulnerable individuals (although they should if they want to be GDPR compliant). They require more education on this topic. As Edward (Research Fellow at UK university) mentioned, mandatory training is essential but training from outsourced companies, which 'fosters antipathy and is seen as a mechanical task' rather than a true learning experience should be avoided. Several interviewees also suggested to raise awareness among consumers and citizens so that they start demanding ethical developments themselves and understand data processing practices better. Hazen (Founder of UK SME) who developed a whole architecture for more privacy-preserving smart homes underlined the importance of educating the public, a necessary pre-condition for them to become more interested in his products.

Interviewees regularly mentioned the need of more guidance, guidelines and codes of conduct, both those working at IoT companies and researchers. As stated in the previous chapter, they can be useful tools for companies to demonstrate GDPR compliance and for regulators to ensure the application of data protection provisions. Experts underscored the lack of enough sector-specific codes of conduct (for the IoT sector), guidelines from DPAs concerning vulnerable individuals in general (which would increase the possibility of taking vulnerable adults into consideration by companies in their processes, in addition to children) and advice

[432] Luna (n 22).

on how to include vulnerability into DPIAs. Neda (Professor of law at EU university) and Charlotte (Researcher at US university, Educator on IoT) criticised slow progress at EU level and made reference to the EDPB's plans to issue guidelines on processing of children's data that never came into fruition. Avena (DPO at UK charity) said that not many organisations will admit to that, 'the privacy sector takes itself pretty seriously' and they 'like to be regarded as the experts of things' but that the reality is that these are still beginnings of the GDPR and 'basically a lot of us are making stuff up'. All of these statements show that guidelines are too scarce. For example, guidance on the most common vulnerabilities in the data protection context could be useful if published by the right actors as it would potentially lead IoT companies to include those vulnerabilities into their data protection work and products.

Finally, enforcement is another necessary aspect of an effective vulnerability-aware approach. Enforcement has been discussed throughout this thesis, in various sections, as without it the GDPR would never become effective. Discussions with interviewees seem to suggest that smaller companies and local authorities have been especially afraid of potential fines DPAs could impose on them. However, according to Aland (CEO and Senior Information Regulation Officer), it is the big organisations that DPAs will go after and not smaller ones that 'interpreted something slightly wrong but with all of the best intentions'. Such opinions might come from the fact that enforcement actions are indeed scarce at the moment and DPAs are typically underfunded (as previously mentioned in this PhD).[433] Most interviewees underlined that enforcement is currently unsatisfactory. For example, Neda (Professor of law) stated that enforcement is a real problem and that vulnerable individuals have not been sufficiently on the agenda of DPAs, but that they are slowly becoming more aware of children-related issues (she gave the example of the Irish DPA's investigation into processing of children's data on Instagram).[434] However, apart from pointing this out, interviewees did not suggest any potential solutions, which could mean that changing the current enforcement landscape while necessary will also be difficult unless there is a political will to do so. One interviewee representing a big organisation providing, among others, support to vulnerable individuals through smart devices, self-declared to the DPA that they made some mistakes in implementing GDPR provisions and they were not sanctioned in the end, due to what was considered as attenuating circumstances.

[433] Veale, Binns and Ausloos 105 (n 117).

[434] Data Protection Commission, 'Data Protection Commission's two statutory inquiries into Facebook's processing of children's data on Instagram (opened in Sept 2020)' (19 October 2020) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commissions-two-statutory-inquiries-facebooks-processing-childrens-data-instagram> accessed 1 July 2022.

How such an approach to enforcement could promote or hinder GDPR compliance is another question requiring further research. In any case, self-declaring violations to rectify the situation as quickly as possible should be supported in one way or another. This might potentially promote greater GDPR compliance when vulnerable people use smart products. In general, it seems that more research should be conducted on current enforcement measures, their effectiveness and how they affect IoT companies as well as people's rights.

3.3.IV An Approach Beneficial to All Data Subjects and Data Controllers

Interviewees reiterated what this PhD emphasised in the previous chapter, which is that if a vulnerability-aware approach was adopted, this would benefit not only vulnerable individuals but all data subjects. For example, for Joline (Senior Research Analyst at UK company), just because information is communicated in simple language does not mean that it would convey less than to a non-vulnerable individual, 'so that could be the standard'. According to Finlay (Research Associate at UK university), if less data is processed due to special measures adopted for vulnerable individuals using a smart product, this would also increase companies' GDPR compliance in general for all individuals. Brennan's (CTO) organisation strives to take special measures for a general population that may include vulnerable people as 'a principle of inclusive design and digital inclusivity'. Promoting such approaches through awareness, education, enforcement measures, guidance, guidelines and codes of conduct is currently needed. How do experts implement and perceive legal GDPR compliance challenges in the context of vulnerable people and IoT devices?

Section 3.4 Legal GDPR Compliance Challenges for Companies and Professionals

This section is divided into five parts presenting the analysis of experts' experiences and views on legal GDPR compliance challenges, namely: professionals' suggestions and implementation of Art. 5.1 (a) GDPR on lawfulness, transparency and fairness (3.4.I); risks of data overcollection, tension with device usefulness and GDPR compliance, all in the context of the data minimisation principle (3.4.II); DPbDD as a sometimes misunderstood concept but crucial element of the GDPR (3.4.III); DPIAs as multifaceted instruments of evaluating risks (3.4.IV); uncertainties around certification and standards (3.4.V).

3.4.I Implementation of Article 5.1 (a) GDPR: Lawfulness, Transparency and Fairness

According to Art. 5.1 (a) GDPR, personal data needs to be ‘processed lawfully, fairly and in a transparent manner in relation to the data subject’. Most professionals are critical towards consent both from a company’s and vulnerable person’s perspective while being more open to adopting legitimate interests, performance of a contract and other legal bases (3.4.I.A). IoT organisations try to achieve transparency with varying degrees of effort and experts provided advice on how to improve this (3.4.I.B). Fairness is currently an underutilised but promising and essential principle in the context of vulnerable individuals using smart products (3.4.I.C).

3.4.I.A Consent as a Mostly Criticised Legal Basis as Opposed to Other Legal Grounds

What kind of legal ground is preferred by companies and how do they implement them? What are the potential benefits and issues linked to the various legal bases in the context of vulnerable individuals using smart products according to professionals? Discussions with experts confirmed a sometimes unproper implementation of GDPR provisions by companies in relation to legal grounds’ requirements and the associated lack of effective protection of vulnerable people’s data (such risks were mentioned in Chapter 2, for example, in relation to the balancing exercise when organisations use legitimate interests). How to prevent those violations was also briefly discussed in the doctrinal chapter, for example, by proposing collaborative work of designers and regulators to create tools permitting quick discovery of GDPR infringements.[435] The empirical study further underscored the need of technological practical solutions, some of which will be proposed in Chapter 4 (on privacy enhancing technologies and personal information management systems).

Concerning consent, professionals and experts’ had mixed feeling towards this legal basis, most of them criticising it, the only positive side of consent mentioned being that it could give more control to data subjects. Firstly, from a company’s perspective, some interviewees stated consent is the last legal ground they would recommend an organisation to adopt, considering

[435] Nouwens and others (n 65).

its requirements are difficult to satisfy, especially when obtaining consent from vulnerable people such as ‘individuals who suffer from mental illness or other conditions that might affect memory, personality, dementia being a key one’ (Damon, UK Solicitor). Moreover, as underlined by Maxwell (Professor of law at UK university), ‘[companies are] going to try not to rely on consent, because they don’t want the data subject to have those rights’ (consent leads to additional legal hurdles).

Discussions revealed that smaller IoT companies are more worried about issues related to not complying with consent requirements as opposed to bigger smart home companies that simply ignore them from time to time. When asked about consent in the context of vulnerable individuals, Farra (UK Solicitor) stated that ‘from a perspective of having in-house counsel it’s never been something that’s come up as a question’, which could mean that IoT companies will sometimes ignore taking special measures in relation to vulnerable individuals while fulfilling consent’s conditions. For Emily (Industry Analyst) consent ‘is a very binary experience where you can either click through and essentially allow the company to collect whatever it wants whenever it wants and also change those terms whenever it wants’. As discussed in Chapter 2, this goes against data protection law, which states that consent needs to be freely given, informed, specific and unambiguous (Art. 4, Rec. 32 GDPR) and that special data protection measures must be taken in relation to children (Rec. 38 GDPR). Violations of GDPR consent-related provisions should be tackled by policy makers and enforcement bodies.

Secondly, statements of professionals show that there is a tension between consent leading vulnerable data subjects to reject potentially useful smart devices (for example, older individuals preferring to reject smart sensors provided by local authorities due to their lack of understanding of data processing intricacies and the resulting worries) and consent as giving more control to data subjects and empowering them to take decisions on their own. Avena (DPO at UK charity) painted consent as a beneficial option as it gives agency to people supported by the charity. To make consent a more meaningful process in this regard, Emily (Industry Analyst) suggested that consent should be more specific, for example, by offering tiered options to consumers, where the level of service received from a device depends on the amount of data you shared with the company, this kind of offering also educating ‘the user on sort of the flow of their data’.

Finally, another consent-related issue important from a vulnerable person's perspective and that this chapter will come back to is age identification online. As Neda (Professor of law) stated, they 'have found it quite difficult to find conclusive research findings about the extent to which a provider can actually say, well, this is the voice of a child. So, for this voice I need to ask for consent from parents'. In that regard, it could be argued that children's data is not sufficiently protected if they cannot be identified and prevented from consenting in potentially harmful situations. As discussed in Chapter 2, not only are age-assurance mechanisms in early stages of development but there is also a conflict between some of those mechanisms and compliance with the GDPR as they may pose a risk of 'intrusive data collection'.[436] This topic will be further elaborated upon later in this chapter.

Legitimate interests has been presented as a more popular and useful legal basis in comparison to consent by a few companies and professionals, one reason being that (according to them) it will result in less GDPR compliance issues (no need for companies to satisfy all consent's requirements mentioned previously in this study). Aland (CEO and Senior Information Regulation Officer) maintained that the most popular model is the non-consent model, where the local authority (his company's customer) does not ask for explicit consent for a particular sensor or a particular product for an individual but rather relies on its duty of care and the 'best interests of the individual'. Damon (UK Solicitor) argued that legitimate interests is popular as it avoids a lot of the issues with consent and 'it could work in those situations where consent is transitory or affected by the fact that somebody has dementia and they may consent in one moment, withdraw consent in another'.

In terms of its effects on vulnerable people's rights, it seems that the benefits of legitimate interests will mainly depend on the company's goodwill. As mentioned by Damon (UK Solicitor), 'you would have to go further to take vulnerability into account when you're doing that balancing act'. Legitimate interests permit data processing in the interests of the individual, taking into account all the elements of their condition, which could be beneficial for vulnerable individuals. However, while this may be true, Neda (Professor of law) added that providers are often not very transparent about the extent to which they have actually gone through this balancing exercise. The extent to which legitimate interests will achieve its aims as a legal

[436] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' 35 (n 26).

basis currently depends on many companies' willingness to truly satisfy its requirements, until enforcement of legal provisions becomes reality. This confirms the findings from the doctrinal study in Chapter 2 and some solutions will be proposed in the fourth chapter.

Concerning performance of a contract, it has been described by Damon (UK Solicitor) as one of the most commonly used and least problematic legal grounds, and that in this case companies usually do not even know that they are interacting with a vulnerable individual. This reduces data protection compliance issues. Maxwell (Professor of law) would 'probably suggest contractual necessity' whenever possible to companies if he was thinking about their interests as a priority. However, Neda (Professor of law) pointed to the fact that this legal basis is 'in relation to one member of the household'. It could indeed be an issue if one member of the smart home purchases the product but the same product is used, for example, by a child for whom the services might need to be restricted or provided on the basis of another legal ground.

In terms of vital interests, the representatives of companies who were interviewed in this study did not use this legal basis. Brennan (CTO) argued that 'because we do preventative care, vital interests probably we would never come across'. Damon (UK solicitor) added that in his experience vital interests is construed very narrowly, 'it's more of a life-and-death type situation'. Smart devices could, for example, share information directly with medical personnel in this type of circumstances. This also confirms the findings of Chapter 2.

In general, all of the interviewees were the most vocal (and rather critical) of consent. Legitimate interests, performance of a contract and vital interests were only briefly mentioned in the discussions but the first two seem to be the most popular for companies developing smart products. For vulnerable consumers' rights, all those legal bases would be much more beneficial if there was true GDPR compliance, for example in relation to informed consent.The latter is linked to the transparency principle, which will be analysed in the following section.

3.4.I.B Transparency as a Difficult but Crucial Principle

As discussed in the previous chapter, the GDPR transparency principle requires organisations to adopt special measures when they communicate information to vulnerable individuals due to the fact that their needs may differ from other citizens (Art. 12 GDPR). How is this requirement implemented by organisations developing smart products?

It results from the interviews that companies still struggle with providing enough transparency and sometimes seem to misconstrue GDPR requirements in this regard (while providing enough information is certainly part of transparency, making sure that vulnerable individuals understand it is as important). This is exemplified by the contrast between Damon's (UK solicitor) and Brennan's (CTO) approach.

Brennan asserted that he doesn't 'find it particularly difficult' to communicate transparently with his customers and that his company goes 'a little bit further than we have to necessarily because we do disclose, you know, all the processes or the sub-processes that we're using through a transparency perspective' but that once they go this far 'individuals just don't care anymore than that', the latter's level of interest being exceeded before the company exceeds the amount of information that could be given. However, GDPR compliance in the context of vulnerable individuals is not only about how much information you convey, what is most essential is how this is done. Brennan's approach contrasts with the opinion of Damon (UK solicitor) who said that achieving transparency is 'one of the biggest challenges for companies, full stop'. The latter added that he will often see privacy policies, which are still written in quite technical language, 'large forms and with a lot of little tiny text', not explained clearly enough and that when vulnerable adults are added into the equation, it becomes even more difficult to convey relevant information. Damon and Brennan came to different conclusions possibly because the latter does not put enough emphasis on the way information is communicated and instead focusses on the amount of information provided to an individual. Damon worked with many companies and, according to him, they rarely adapt communication mechanisms to the needs of vulnerable customers.

In this context, Aland's (CEO and Senior Information Regulation Officer) company has created a braille version for a visually impaired person. However, this happened only after being explicitly asked to provide such a version proving that it would not exist otherwise. This is an important reminder of the need to adapt transparency measures to various types of vulnerabilities and not only to children.[437] While measures adopted for children will certainly

[437] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (n 173).

increase transparency for everyone, they will not be sufficient. Possibly, with the right guidance and enforcement, all products could be adapted to the most common vulnerabilities. Currently, this does not seem to be the case.

Interviewees proposed to improve transparency measures through means such as gamification, easy-read material, videos, adapting communications to various kinds of vulnerabilities by default and including vulnerable individuals in the design of transparency measures. For example, Avena (DPO at UK charity) stated that while people with learning disabilities can be helped through technologies such as IoT products, they often cannot understand the legal ramifications of what they agree to and should be provided easy-read material to be able to do so. Emily (Industry Analyst) suggested that 'the privacy conundrum in which we live is actually a user interface issue' giving the example of chatbots, some of their communication processes being 'so frustrating and confusing' leading people to just click through and accept everything to get to the actual use of the service. Kismet (Researcher at EU university) mentioned involving 'children in the design and creation of these information formats' as essential, something that has already been proposed in legal literature and mentioned in Chapter 2.[438] These kinds of research endeavours could result in the development of best practice guides on how to write and communicate data related topics to children and vulnerable adults. Some progress in this regard has been made through the publication of ICO's Age Appropriate Design report.[439]

Transparency has not been explictly linked by experts to the publication of DPIAs, DPbDD measures, certifications, codes of conduct or other mechanisms (as proposed in Chapter 2) so professionals assume that discussing transparency mainly means discussing the way information is presented rather then new channels and actions through which it could be communicated.

3.4.I.C Fairness as a Useful but Vague Concept

This thesis will now discuss the fairness principle and how professionals perceive it in the context of vulnerable individuals and smart products. Firstly, most interviewees agreed that

[438] Donoso, Van Mechelen and Verdoodt (n 179).

[439] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' 37 (n 26).

fairness is not effectively applied or used at the moment due to problems linked to its definition. Farra (UK Solicitor) compared fairness to the concept of vulnerability and difficulties in defining the latter, which then leads to problems with its application in practice. She added that she attended a workshop and they were discussing 'all those different types [of fairness] and you think, okay well it could be, the GDPR could be any or all of those'. Finally, Farra contended that many academics say that it just doesn't exist at the moment 'which is not overly helpful to us [professionals]'. For Maxwell (Professor of law), courts also need to give content to fairness when this principle is violated. Maxwell stated that because of its flexibility and adaptability, fairness might be 'the most important principle of the GDPR'. Any attempt to define it would be useful. Joline (Senior Analyst) linked fairness to non-discrimination and bias in the context of AI and smart devices but considered it difficult to actually explain what fairness means in practice. Similarly, Neda (Professor of law) said that fairness 'is always quite vague' but could be linked to the best interests of the child, 'one of the key principles in the United Nations Convention on the Rights of the Child'. According to Maeve (Senior Research Analyst at UK company), the concept of justice is more often used by academics as it is 'something more tangible' than fairness. It's often elusive within DPIAs and it's difficult to 'force the developers or the companies' to integrate it into their systems. Maeve discussed her project of a 'human rights impact assessment' in order to make human rights easier to implement by business and proposed to associate fairness with more concrete concepts like human rights. She added that just like privacy is more than data protection (to implement the former 'breaking it down into smaller parts like data protection' was necessary), the same should happen with other complicated concepts like fairness.

While fairness may be difficult to define, it is included in the GDPR and as this thesis has mentioned in the doctrinal chapter, it is essential to works towards defining this concept as it could be especially useful in the context of vulnerable people's rights when they use new technologies such as smart devices. The interviewees' responses show that while it is a vague concept, professionals and researchers have diverse ideas on how it could be defined. A larger debate and the development of analytical frameworks by academics, courts and regulators are needed to make the fairness principle more tangible and applied by professionals.

3.4.II Data Minimisation

There is a tension between the usefulness of some smart devices for vulnerable individuals and data collection (3.4.II.A). While there may be situations in which data collection is necessary, there are also increasing risks associated with the overcollection of data, especially for vulnerable individuals (3.4.II.B). Companies seem to comply with the data minimisation principle to varying degrees. It would be beneficial for them and vulnerable persons' data protection to increase the level of their compliance (3.4.II.C).

3.4.II.A Tension with Device Usefulness

Discussions with interviewees have shown that a tension currently exists between data minimisation and the usefulness of some smart products for vulnerable individuals. Whether these are related to education, entertainment or health, smart devices can bring opportunities and benefits to children and vulnerable adults[440]. However, both chapters 1 and 2 described the important risks of GDPR violations linked to IoT products considering the excessive data collection practices often associated with their use. There are two main reasons for which interviewees justified the necessity to collect vulnerable people's data. Firstly, several persons underlined the importance of increasing the capacity of smart devices useful for vulnerable individuals in their daily lives. As Aland (CEO and Senior Information Regulation Officer) and Brennan (CTO) contended, collecting vulnerable individuals' behavioural data is in the general best interest as it allows to develop products allowing better services and treatment. According to Lari (Senior Research Fellow), there is a need to develop these sort of devices in aged care because they're going to be 'efficient and cheaper and give people better quality of life'. In relation to children, Neda (Professor of law) reflected on whether there could be a possibility for smart devices such as voice assistants not to record children's data at all but then stated that they would lose some functionality and that 'smart devices are often used by children for their benefit as well, for educational purposes or entertainment purposes'. A second reason to collect vulnerable people's data (and linked to the former due to the necessity to improve such systems) is in the context of exceptional circumstances, for example, when their health could be at stake (it could be to detect falls and increases in frailty). This has also been discussed by several interviewees. Hazen (Founder of UK SME) remarked that 'I also hear these situations, where because they had Alexa or Google Home they were able to call for

[440] Ingrida Milkaite and Eva Lievens, 'The Internet of Toys: Playing Games with Children's Data?' in Giovanna Mascheroni and Donell Holloway (eds), *The Internet of Toys: Practices, Affordances and the Political Economy of Children's Play* (Palgrave Macmillan 2019) 285.

help'. Maxwell (Professor of law) underlined that while data minimisation is an important principle in general, it shouldn't prevent companies from processing information, which would allow 'to tackle the vulnerability of the individual'. Joline (Senior Analyst) even argued that in some cases, this 'goes beyond just legal compliance', 'because the purpose of these things is actually noble I'd say'. These situations do not necessarily need to be health related. Emily (Industry Analyst) underlined the importance of certain apps designed for the elderly to help them manage financial services. She argued that elderly folks are often targeted with online fraud and while it might feel like they are sharing a lot of data with a company, it could be a way for the latter to better protect their online footprint. This points to the need of privacy-preserving systems, which would allow both data minimisation and development of useful products as well as providing help in difficult circumstances. Charlotte (Researcher and Educator) mentioned seeing research about how to identify a person who has fallen by monitoring them but keeping this data as private as possible. She said such solutions are a question of time as there is 'a viable use case'. While collecting data may have benefits in certain circumstances, what are some of the risks linked to data overcollection for vulnerable individuals using smart products?

3.4.II.B Risks of Data Overcollection

Emily (Industry Analyst) provided several interesting examples of risks related to vulnerable individuals and data overcollection through new technologies. Firstly, vulnerable persons are often targetted for fraud-related reasons, for phishing, cybersecurity scams and there are 'so many unbelievable uses of emerging technologies' such as hackers using chatbots to build trust with a user and 'to say, hey, this is your kid, I'm texting you, I'm in need, send me a million bucks, or whatever'. For this reason, if vulnerable people's data is publicly available in an increasing number of places, they could become easy targets for cybercriminals. Data minimisation seems especially relevant in their context.

Another example is digital phenotyping, which is an emerging practice whereby biometrics, health outcomes, behavioural tendencies and other sensitive information could be inferred through seemingly irrelevant data. According to Emily, by using keystroke analytics (how long someone hovers over a website, how fast someone types or which emojis they use), some companies categorise people into various health states such as depression or Parkison's disease and marketing analytics firms use this information for behavioural targeting. The implications of these inferences can be damaging for vulnerable populations such as older people who ‘might not be comfortable typing as quickly as you or I, they might not even use emojis’. These risks are linked to excessive vulnerable people’s data collection when they use products such as IoT devices.

The rise of biometrics, especially for older people or for persons with particular health conditions, introduces new privacy concerns as they could be shared with potential employers, with health insurance risk modelers or with credit and loan services. Emily warned that the same techniques, which were used for advertising to infer knowledge about individuals, could now be used for emotion, for health, for mood or for politics. In general, this overcollection of data seems especially dangerous for children and vulnerable adults. It is for this reason that this thesis considers data minimisation as a particularly relevant principle in the context of vulnerable persons using smart products.

3.4.II.C Compliance Approaches and Solutions to Data Minimisation

This thesis will now analyse how data minimisation works in practice. As one professional framed it:

> If you don’t need information about their condition or their vulnerability, then you shouldn’t be recording it. It should only be if it is necessary and relevant in order to do the additional processing you’re going to be doing. Particularly with vulnerable individuals as well, a lot of the time that information will be health data and therefore it will be special category personal data so you’re then needing an additional legal basis under Art. 9 of the GDPR in order to process it in the first place, it increases the risk to the individual, so you’re back onto the high-risk tests if you’re considering things such as reporting to the ICO, notifying data subjects, doing a DPIA, for example, all of those things become a lot more complicated and a lot more in-depth. The level of appropriate technical and organisational measures you use for the security around the data, those will be higher when you’re starting to record that special category data. So, if you don’t need it, you shouldn’t be recording it. (Damon, UK Solicitor)

In short, the less information is processed, the fewer data compliance issues a company will need to face, especially in the context of special category data often gathered from vulnerable individuals.

While most interviewees simply stated that they strive to collect as little data as possible, Brennan (CTO) provided more information. He increases his devices' compliance with data minimisation when the commercial sector is involved but collects more data when his company collaborates on a research project within a 'strong ethics environment'. According to him, almost anything can be inferred with the right approach from data collected through his wearable smart devices. It is interesting to note Brennan's trust in the research sector in comparison to the commercial one, and his assumption that vulnerable persons' data will be used to influence consumers' choices within the latter. Moreover, this shows that companies currently choose who they consider trustworthy enough to send more data to. The fact that this 'is very useful research' might have also tipped the balance in favour of collecting more data for research purposes. The data minimisation principle is overarching and there shouldn't be such a big difference between the amount of data collected by one organisation over the other, unless there is a compelling legal ground justifying this difference.

Hazen (Founder of UK SME) created a smart home edge-based architecture that allows companies not to store any customer personal data, which means that they wouldn't need to worry about most privacy laws if they used his system. He underlined that it is important to focus on vulnerable people in this context, 'as those are the ones who would not even know that the data is going out'. If Brennan was able to process all this data inside his vulnerable customers' homes as Hazen suggests, especially in the context of his more data intensive research projects, he could potentially avoid data compliance-related risks and still improve smart devices and acquire more knowledge on how to support vulnerable individuals. This alternative technological model will be analysed in more detail later in this chapter and comprehensively in Chapter 4 of this thesis.

Limiting data processing time is another potential option for increasing compliance with the data minimisation principle. Beth (Senior Vice President) stated that there are companies developing mechanisms where customers can choose the amount of time for which data will be stored on devices. Such time limitations could also be applied to companies' data processing activities to better comply with the GDPR.

Emily (Industry Analyst) argued that a lot of companies are in a hoarding mindset, ‘the more data I can get the better’, but that when it comes to GDPR, and particularly in highly regulated industries, having a hoarding mentality ‘does not lend itself well to a very clear and up to date data inventory, which is absolutely part of several different compliance regimes’. What Emily suggested was that data minimisation can lead to more effective processes, less potential compliance issues and higher customers’ trust in the organisation, potentially benefitting them financially too.

Finally, some interviewees stated (similarly to this thesis in Chapter 2) that the principle of data minimisation is crucial for everyone, not only inherently vulnerable data subjects, especially considering the various layers of vulnerability a person may possess. Minimising data collection and processing is an essential process that would benefit all consumers of smart products.

3.4.III Data Protection by Design and by Default

Data protection by design is beneficial both for vulnerable individuals and companies to facilitate GDPR compliance (3.4.III.A). However, some experts still seem to lack expertise on DPbDD and some issues remain, for example, in relation to how data protection by default measures are implemented by IoT companies (3.4.III.B).

3.4.III.A Data Protection by Design as Essential for Vulnerable Individuals and Beneficial for Companies

Considering the fact that DPbDD is an overarching principle (as discussed in Chapter 2), essential for the implementation of all GDPR principles, by design measures are certainly both an opportunity and a challenge to ensure greater GDPR compliance.[441] Maxwell (Professor of law) stated that ‘bad data protection by design is actually really dangerous’ as rules are being written into the code and it cannot be easily changed later, especially in the case of hardware designs. As will be discussed below, a by-design approach would not only increase vulnerable

[441] EDPB, ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default’ (n 173).

individuals' data protection but it would also intrinsically enhance organisations' GDPR compliance.

Data protection by design was mostly linked by interviewees to limiting data collection (so also data minimisation) and security measures. As Emily (Industry Analyst) noted, decisions need to be taken as to what sensors go into the device, whether it is connecting to a router or whether everything goes back to the cloud. These choices are crucial for GDPR compliance and are overarching. Limiting data collection is indeed what could help the most in terms of protecting vulnerable people's personal data. Sophia (Founder of a charity, start-up and Head of Developer Relations) stated in relation to children with autism that 'they wouldn't care if somebody is stealing their information or using a camera to capture them' as they are often not aware of what other people can do to them. They will not read policies and will 'definitely always press the agree button', so for these individuals, security by design is essential. Indeed, without data protection by design, some vulnerable persons' data could be more easily abused than that of other citizens.

However, previous chapters of this thesis have shown that data protection by design is not only about security and data minimisation. It is also essential, for example, in the context of transparency. Laine (Researcher at UK university) argued that the problem lies in the variety of vulnerabilities people can represent, 'because how do you design for an almost uncountable amount of different variables that could come in this?' While this concern is valid, implementing effective by design measures, such as interfaces adapted to the most common vulnerabilities or technological architectures minimising data collection, would still be beneficial (even though not perfect) for all vulnerable individuals and would be a big step forward when compared to current practices.

Apart from benefits related to greater GDPR compliance, for companies, data protection by design can be a useful way to convince consumers to buy devices. According to Edward (Research Fellow), if Apple 'comes along and says, for five bucks a month, you get full access to our ecosystem, but your data is as safe as we can make it and we are never going to dip into it', that could be 'a serious decision maker' for him and an encouraging step in the right direction.

3.4.III.B Experts' Knowledge of DPbDD and the Application of by Default Measures

It seems that there is still not enough knowledge of what DPbDD entails among IoT professionals. The question of terminology and differentiating between by default and by design measures is an issue for some professionals. When asked about DPbDD, Aland (CEO and Senior Information Regulation Officer) and Brennan (CTO) were not certain of what this exactly means. Brennan preferred the notion of privacy by design to DPbDD. He explained that DPbDD 'is not a particularly useful concept' beyond privacy by design and that he finds it 'damaging when people start to try and confuse the issue by being clever about what different things mean because it's just not helpful'. He added that 'privacy by default is a get-out clause for organisations that haven't yet managed to do privacy by design'. This shows that the GDPR is not sufficiently understood within certain companies. Brennan's organisation is producing smart home devices used by vulnerable adults and it can only be GDPR compliant and adequately protect vulnerable people's data if DPbDD is properly implemented.[442] For this to happen, it is essential that all terminology is correctly comprehended and defined.

Perhaps surprisingly, not many interviewees mentioned data protection by default measures whereas this thesis argued in Chapter 2 that they are essential in the context of vulnerable adults using smart products. Maybe, data protection by default is still sometimes conflated with data protection by design as Brennan's interview seems to indicate. Aland indirectly criticised data protection by default stating that when vulnerable people have the option to opt in or opt out, this can confuse people and they might choose the opt out option while 'it's absolutely in the interests of everybody if everybody opts in'. His company is producing smart health devices used within people's smart homes and it seems that he prioritises data collection over individuals' awareness and agency. However, this is opposite to what the GDPR suggests and, as a result, not GDPR compliant.

Depending on how it is presented, data protection by default can positively or negatively influence vulnerable users of smart devices. The way by-default measures are currently implemented is often not neutral. Beth (Senior Vice President) worked at some of the biggest IoT organisations and stated that companies tend to influence consumers by suggesting that they will lose out if they don't opt in whereas 'people don't really understand the opposite side

[442] Hildebrandt and Tielemans 517 (n 276).

of the equation', which is unfair. This is especially relevant in the context of vulnerable individuals and to what Sophia (Founder of a charity, start-up and Head of Developer Relations) said about some individuals with autism, namely that 'if you give them let's say a dialogue box asking them, do you agree – do you want to proceed, your information is being captured? Press yes to approve, no to deny', they will simply agree to what gives them the easiest access to the service. It is important to implement data protection by default in a way that prevents automatic opt-in choices. Beth mainly discussed opt-out as being an option that the consumer needs to actively choose, indirectly suggesting that there are still companies not implementing data protection by default measures and consumers needing to actively opt-out, which is of course a major GDPR compliance issue. While there certainly needs to be more customer awareness in terms of both benefits related to opting-out and opting-in, as argued before in this thesis, opt-out settings by default are essential for vulnerable individuals who may not be always interested or capable of learning about unnecessary data processing in detail and simply want to safely use the service that their smart device is supposed to offer.

3.4.IV Data Protection Impact Assessments as Multifaceted Instruments of Evaluating Risks

DPIAs are crucial for vulnerable people as they may be one of the main instruments increasing the chance that companies will take their needs and rights into consideration at an early stage of smart product development and deployment. As explained in the previous chapter, DPIAs are required by the GDPR when vulnerable people use smart devices as this represents a situation that could result in high data protection-related risks. This thesis will discuss how professionals conduct DPIAs before analysing suggestions on how they could be improved.

Avena (DPO at large UK charity) stated that her organisation has a great DPIA template, which has been commended by the ICO. The template looks at every principle, every data subject right and security measure, and it is not just a tick-box exercise. Every project this organisation undertakes must pass the DPIA otherwise it is not implemented. As this charity directly works with vulnerable persons, their DPIAs need to take their righs into account. There is a potential opportunity here for the ICO to work with organisations like Avena's and engage with them to gather insights, for example, when preparing new guidelines. Other organisations, such as smaller charities and companies working on IoT projects, would certainly benefit from such templates as they may not possess the same experience and resources. This is also what has been suggested by Maxwell (Professor of law) and Neda (Professor of law). Brennan (CTO) considers that if we 'look at most of the devices that are out on the market in the consumer space, the risk profiles are horrific', suggesting that most organisations do not do DPIAs effectively enough.

Hazen's SME used a cyber security consultancy to support them in DPIA processes. While this may at first view lead again to the conclusion that smaller organisations need more guidance and support as they cannot do this internally, the practice of using external independent experts to conduct DPIAs is not an inappropriate measure. Conducting DPIAs by internal privacy officers could result in a conflict of interests and external independent experts may be a more suitable choice in certain circumstances, as they could potentially be more objective in their conclusions and recommendations.[443] The negative side is that they might not be familiar with, for example, the needs of vulnerable individuals for whom a smart product has been developed or they might see this exercise as too narrowly focussed on data protection and security, ignoring all the societal aspects and values linked to the place and nature of data processing, whereas the company developing a smart device will be more familiar with those issues and the overall setting of its activities. However, DPIAs can also be done through a collaborative process involving both the external organisation and the IoT company to produce the best results possible. This process will depend on the willingness of the IoT business to be involved and how comprehensive it wants the assessment to be.

What are professionals' opinions as to how DPIAs should be conducted? Interviewees' responses seemed to more or less align with this PhD's suggestion to consider the rights-based and values-oriented impact assessment model proposed by Alessandro Mantelero (or at least to go beyond data protection considerations).[444] Maeve (Senior Analyst) thought important to move beyond 'the DPIA to this PIA+ [privacy impact assessment]'. According to her, current DPIAs cannot sometimes catch more difficult concepts like fairness and do not succeed in integrating them into companies' smart products and systems: 'data protection laws do not cover other ethical and social issues that might emerge from the development and the employment of digital technology'. Certainly, from the perspective of taking special measures

[443] Gonçalves 147 (n 328).
[444] Mantelero (n 330).

for vulnerable people (for example, Rec. 38 GDPR) or the fairness principle, PIA+ would make organisations' processes more GDPR compliant. Similarly, Kismet (Researcher) declared that DPIAs should consider children's best interests, not only their rights to privacy and data protection but also other rights of the child and the ways they may be affected when their personal data is processed by smart devices. In this context, Neda (Professor of law) remarked that children's rights impact assessments (CRIAs) exist for a long time now (for example, UNICEF conducts them) and they could be implemented or integrated into DPIAs.

Several interviewees thought that organisations should involve vulnerable adults and children in DPIAs if this is possible and regularly (re)assess DPIAs with them. For example, Joline (Senior Analyst) stated that it's important to have vulnerable people's voices heard because it will ultimately affect them and they can give 'different insights from just developers or the kind of legal compliance people into ways they could suffer or view risks and harm'. However, Joline added that at the same time certain things that make people vulnerable mean that their engagement with the process of how tech is used might not always be so useful. Sometimes, it might be difficult to ask a child or vulnerable adult to participate in the process because they might not have the technical knowledge or be able to fully express their opinions, for example, due to their medical condition or to the difficult situation they are in (Joline was working on a victim identification facial recognition app, a very sensitive project). She mentioned that carers, such as doctors, would be a good alternative and that they could be involved in DPIAs as well. Of course, this is assuming organisations have the resources to include vulnerable people or their legal guardians in their DPIAs processes in the first place. Guidance from those that have done so would be valuable for companies that were not able to involve vulnerable persons or their carers' perspectives despite their best intentions.

3.4.V Uncertainties Around Certification and Standards as Compliance Tools

This section confirms some of the findings and hypotheses from Chapter 2 in relation to the lack of implementation of standards and the potentiality of improving compliance through certification and labelling schemes. Firstly, in the doctrinal chapter, this thesis asserted that many organisations do not implement effective standards or ignore some of their requirements. The fact that only one interviewee, Aland (CEO and Senior Information Regulation Officer), mentioned specific ones used by his organisation seems to confirm this. His company uses

Cyber Essential Plus and the QSF standard.[445] They mainly cover security processes (such as two-factor authentication). Aland stated that there are 'various people suggesting various things, but there is no hard-and-fast rulebook as to what you need to do' in terms of standards and certifications. Both this chapter's findings and other empirical studies suggest that standards are currently often inconsistent, issued by various bodies and implemented in different countries, and their harmonisation seems necessary to resolve this problem.[446] As mentioned in Chapter 2, harmonised standards are considered by the CJEU as part of EU law, which greatly increases their potential for implementation in practice. Currently, smart home companies seem to mostly rely on security standards, some interviewees declaring that there is a need of standards and certifications more specifically focussing on data-related issues and vulnerable individuals.

Secondly, in Chapter 2, this thesis advanced the idea that the lack of implementation of effective standards may be due to potential costs, which organisations want to avoid or simply because they do not see any incentive to comply with them (for example, due to the above-mentioned fragmentation and lack of clarity as to which standards should be implemented). While those points seem to be interlinked, interviewees underlined the former. For example, Maxwell (Professor of law), explained that he interviewed several IoT designers who were working on an open IoT certification scheme but ultimately gave up as they felt that this would create too many obstacles to entry to the market and only the big companies would be able to afford compliance with these standards. New certification schemes announced by the government and industry (mentioned in previous parts of the thesis) should take this into consideration during their development[447]. There is a myriad of small IoT companies doing important work for vulnerable individuals and standards should support their compliance efforts as opposed to excessively hindering their processes.

Thirdly, this thesis previously argued that certifications can not only increase GDPR compliance (for example, in relation to the transparency principle) but also increase customers' trust in products and companies. However, the assumptions upon which they are based and the

[445] TSA, 'The Quality Standards Framework' (2022) <https://www.tsa-voice.org.uk/-covid-19/safe-working-environments/quality-standards-fr/> accessed 1 July 2022; ID Cyber Solutions, 'Cyber Essentials Plus' (2022) <https://cyberessentials.online/cyber-essentials-plus/> accessed 1 July 2022.

[446] Chen and Urquhart 117 (n 389).

[447] See, for example, DCMS, 'Consultation on the Government's Regulatory Proposals regarding Consumer Internet of Things (IoT) Security' (n 218); BSI, 'BSI Launches Kitemark for Internet of Things Devices' (n 398).

criteria against which they are evaluated need to be carefully thought-through. Many interviewees shared similar thoughts and further elaborated on what would be needed to ensure the effectiveness of certifications: independent monitoring bodies, effective enforcement mechanisms, trustworthy certification bodies and flexibility of certifications to adapt to rapid technological change. It is in the interest of both companies (higher trustworthiness) and vulnerable individuals (higher probability that certifications signify effective compliance) that certification bodies are well selected (what this means should be evaluated in further studies). Edward (Research Fellow) affirmed that he would use devices with a sticker proving that they are privacy-preserving 'all the time'. As other interviewees mentioned, those certifications would need to come from organisations he considers trustworthy. Certifications should not give a false sense of confidence to consumers.

Section 3.5 The Need of a Privacy-Preserving Holistic Technological Model

Data protection is an inherently interdisciplinary endeavour requiring the participation of both technologists and lawyers (3.5.I). Due to the impossible perfection of security and confidentiality measures as well as dificulties in practically resolving the confidentiality versus control debate, new technological architectures are needed (3.5.II). Technological solutions are also required considering problems linked to the technical identification of vulnerable people and their legal guardians as well as to data co-management processes (3.5.III). A holistic technological model in the form of edge computing could help in finding answers to some legal hurdles when vulnerable people use smart products and better protect personal data in general (IV).

3.5.I Interdisciplinary Endeavour

For most GDPR compliance issues, legal questions are interlinked with technological developments and, as a consequence, lawyers should collaborate with technologists and vice versa to understand new technologies and architectural models (discussed later in this section), and how they can support legal compliance. Farra (UK Solicitor) argued that she worked in the past with computer scientists as she is not 'overly technical' and even though she now has some knowledge and gains more each day, 'it's their domain not mine' and close collaborations will always be necessary to do effective data protection by design. Maeve (Senior Analyst) contributes to the by design approach through impact assessments by bringing legal expertise to more technologically focussed partners and support them in developing tools that follow privacy by design principles. In this regard, this thesis considers crucial for lawyers to be aware of vulnerable adults' and children's rights within the GDPR context (and other contexts) to be able to include those considerations into the by design approaches. Maeve added that currently companies 'have no idea of this kind of literature [on vulnerable groups]' and 'they don't include kids in their design process'. This is not because they are 'mean people' but they do not think about it. This statement points to the need of more awareness and willingness to include vulnerable people's rights into organisations' data protection by design processes. This certainly necessitates an interdisciplinary approach and the knowledge that the GDPR actually requires to take vulnerable people into consideration, including within DPbDD.[448]

The interdisciplinary nature of data protection and GDPR compliance in general is further confirmed by companies' organisational measures. In both Aland's and Brennan's IoT companies, the data protection officer (DPO) is also their chief technology officer (CTO), as in most SMEs (according to Aland) such roles are often combined together. This shows how also in practice, legal compliance issues are intertwined with technological expertise and backgrounds. The DPO position requires extensive legal knowledge and CTOs in those companies should certainly receive specific training in this regard, otherwise there are risks that, among others, only some of the GDPR provisions will be implemented leaving aside the probably less known (but essential) aspects of data protection compliance such as vulnerable people's data protection rights.

3.5.II Security and Confidentiality

No security measures can be perfect (3.5.II.A). In light of these considerations and in the context of vulnerable individuals using smart products, this section analyses experts' opinions on the confidentiality versus control debate and underlines the need of new technological solutions (3.5.II.B).

3.5.II.A Impossible Perfection of Security Measures

[448] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (n 173).

Several interviewees said that security measures can never be perfect and that malicious actors are always lurking around, looking for the next company, which they will attempt to hack and steal people's data from. Aland (CEO and Senior Information Regulation Officer) affirmed that everything is hackable and 'I've been into some quite silly meetings where people say, you know, "you need to make sure it can never be hacked", and that's ridiculous'. As he further explained 'it's a bit like having cameras on your house. It just means that the burglar's going to go to your next-door neighbour with no cameras rather than you. It doesn't make it impossible'. His remark suggests that security measures could have a dissuasive effect (however, a hacker might also treat this as an interesting challenge if security measures are robust). Finally, some companies consider that the more layers of security there are, the harder it will be for them to analyse data. This is not necessarily true but in any case, it is a GDPR requirement (Art. 32) to adopt state-of-the-art security measures and to ensure data is as secure as possible (while also allowing individuals to exercise their rights). There may be a tension within organisations in terms of adopting certain security measures and the company's access to data that those measures could hinder.

Considering what has been mentioned above, in Chapter 1 and in the beginning of this empirical chapter, namely that all data could be personal, that vulnerable people's data can be particularly sensitive and that no security measure can be perfect, the conclusion that this thesis arrives at is that in the context of vulnerable persons using smart products, the biggest problem is data collection. As soon as any data is gathered and processed, problems with GDPR compliance might appear. Of course, there should be some exceptions, for example, if collecting data is currently the only way to help in improving an individual's health, but technological models permitting more privacy-preserving data computation are needed.

3.5.II.B Experts on Confidentiality Versus Control

The privacy-as-confidentiality and privacy-as-control debate was introduced into the question set early in the interview process following one interviewee's mention of this topic. This lead to a variety of responses from different angles. As stated in Chapter 2, this is a theoretical debate, which will be further explored and grounded in legal literature in the more theoretical fourth chapter. It has important practical implications and discussions with interviewees shined a light on how professionals perceive this contentious topic. They served as the basis for a more in-depth analysis in later parts of this thesis.

Firstly, it can be said that professionals prioritise confidentiality, for reasons related to both vulnerable individuals' and companies' perspectives. For example, Farra (UK Solicitor) replied somewhat unsurprisingly that 'knowing the difficulties that you can come across in trying to organise affairs of people who have transient or lack of mental capacity', she would advise her clients to make everything confidential as this is much easier to manage internally. On the other hand, Sophia (Founder of a charity, start-up and Head of Developer Relations) stated that giving control to children with autism 'doesn't really make sense', that security by design 'is way more important' as they will choose whatever gives them the quickest access to the service.

Secondly, as opposed to professionals' approach, researchers underlined that giving control to vulnerable data subjects is mandated by the GDPR and that confidentiality should not trump control by default (and that taking it from them can be seen as overly paternalistic). At the same time, most researchers stated that it all depends on the vulnerability and situation, and that giving control to vulnerable people might not produce the best results for the latter in certain circumstances. The problem is that by design security measures are usually applicable to all customers and not context-specific. The question of how to resolve this conundrum will be explored in Chapter 4.

Interestingly, Neda (Professor of law) discussed control and confidentiality in light of not only the 'very narrow data protection lens' but also other children's rights. Indeed, if we think about all the rights that children have, for example, in the United Nations Convention on the Rights of the Child, they wouldn't be able to exercise them effectively enough if their data's confidentiality was not ensured.[449] While confidentiality may reduce vulnerable people's GDPR control-related rights, it might increase other children's (or vulnerable adults') fundamental rights, such as children's right to express their views freely (Art. 13 of the Convention), which would be impacted if they couldn't do this confidentially in a safe space wihin their homes. How confidentiality and control interact with other rights vulnerable people may have requires additional studies.

[449] Convention on the Rights of the Child (n 4).

Finally, Hazen (Founder of UK SME) presented his view that neither privacy-as-control nor privacy-as-confidentiality are ‘real privacy measures’ and he would avoid taking that route by not getting any data out at all. He explained:

> I think the confidentiality, privacy-as-control thing is more of a gimmick. So, privacy-as-control is more to instruct, telling people, oh you can’t do anything about it, you have to give me your data, it’s just an oxymoron for that thing to say, no, no, you have control. But I don’t think it really serves any purpose in a way. So, when it comes to confidentiality, I mean with Apple they still have access to all your data; Apple, Amazon as well as Google, all three of them admitted that they have real human beings listening to conversations to improve their text-to-speech, speech-to-text recognition. So that defeats the whole purpose of confidentiality, right, because ultimately the concern is, what I speak in my bedroom needs to stay within my home, right, I just – so it’s psychologically hard for me to accept that somebody’s listening for whatever reason that they need.

While the confidentiality and control debate is crucial in the current IoT landscape as well as in the context of GDPR’s provisions and data protection compliance, Hazen has a point by saying that in the cloud computing scenario, there is this element of trust that vulnerable consumers or their guardians must have towards the company they buy products from and that ultimately, if data does not stay where the consumer is located, no one really knows what will happen to it. For Hazen, the main problem is data collection and his privacy-preserving smart home architecture will be explored subsequently in this chapter.

3.5.III Issues with the Technical Identification of Vulnerable Individuals and Design for Co-Data Management

Technological choices can either support or hinder GDPR compliant and safe management of vulnerable persons’ data by their legal guardians and by themselves. One technological issue, which was mentioned several times by interviewees is the difficulty in learning about users’ age (and verifying whether their response are truthful) and in identifying who is using the smart product, whether it’s a vulnerable individual, a legal guardian or another person (such as incidental users), a necessary pre-condition for effective GDPR compliance. In this context, discussions in Chapter 2 of this thesis have also shown that problems related to age assurance continue to exist and there are no adequate solutions.[450] For example, as Lee (Research Fellow at UK university) noted, a child can say that they are above the age of sixteen but they could be any age and 'there's no technology by which that can be verified'. Moreover, the person creating the account is not necessarily the legal guardian of the vulnerable person using the smart product linked to that account. This leads to the conclusion that it is always better to assume, especially for products produced for the general population, that all categories of vulnerable people could use them. However, they should still be identified to, for example, adapt communication mechanisms to their particular needs or understand whether the user is a child and can continue to use a particular service. This problem will be further analysed in Chapter 4 to evaluate how technologies might help in these processes. Interviewees' responses inspired some ideas proposed in the more theoretical and technology-oriented subsequent chapter. For example, Hazen (Founder of UK SME) suggested that edge-based vision systems could be developed, meaning none of the data leaves the device, 'so the frames are directly processed on-device, the information is identified on the device'.

Apart from the issues related to the identification of individuals and their age, interviewees also discussed the topic of co-data technological management, which also inspired Chapter 4's analysis of this subject. There are technological issues related to vulnerable people managing personal data themselves as well as their data being managed by others. For example, one interviewee asked 'what do we do if somebody decides to include [into a device or app] something they don't want to, for example, share with family members?'. Interviewees underlined that IoT companies' assumption is that the person responsible for the account and password protection is monitoring who and how is using the associated smart product. Another potential problem related to this is the abuse of vulnerable people's personal data by other members of the smart home. As Aland (CEO and Senior Information Regulation Officer) stated, 'if somebody wanted to buy an IP camera and stick it into mum's house, they could. The IP camera company isn't going to be held liable because somebody used their equipment to spy on somebody'. Further discussions are needed on how abuse of vulnerable individuals through smart products can be prevented, potentially with some help from new technologies. As Aland mentioned, this is probably not an issue that will be easily solved by IoT companies

[450] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' 35 (n 26).

and their compliance with the GDPR. However, organisations could address some elements of this problem indirectly through the choice of a particular architectural model within which their smart devices will operate.

3.5.IV Challenges and Merits of Edge Solutions

As it was very briefly mentioned in the previous section, edge computing solutions could potentially help with a more privacy-preserving identification of individuals. However, if one looks more holistically at this technological architectural model, what are its challenges and potential benefits according to professionals? This part of the thesis will provide initial ideas (explored in more depth in the next chapter) and evaluate experiences of experts working within the smart home field.

Firstly, this section will analyse interviewees' statements, which underlined edge computing advantages, the main one being local data processing. For example, if no or little data leaves the smart home, companies would need to worry less about the requirements of legal bases such as consent. Beth (Senior Vice President) who worked at some of the biggest companies producing smart devices considers that doing machine learning at the edge is increasingly possible and this should continue to be developed. Emily (Industry Analyst) explained that keeping information at a local computational source has positive effects on security and avoids honey pots, these 'central repositories of sensitive information' in the cloud. Processing at the edge 'reduces the amount of waste, the amount of traffic, the amount of volume' and this leads to tangible economic benefits as 'often companies pay on the amount of distance that the data is travelling'. Moreover, there are reduced connectivity constraints and reduced energy consumption, 'which we all need'. All of those benefits result in greater GDPR compliance. If vulnerable people's data stays within their smart homes, then there will be fewer data protection compliance issues for companies, both from a security and data subjects' rights perspective.

Secondly, another advantage of the edge mentioned by a few interviewees is trust building with consumers. For example, Beth appreciated the fact that Apple focussed more on data being stored at the device level and not going into the cloud, thereby increasing privacy. Emily declared that companies can use this kind of technical architecture as part of trust building, storytelling around privacy and data processing. Following research done with potential consumers, Hazen (Founder of UK SME) mentioned their concerns regarding voice commands going into the cloud and data collected by smart toys in particular. Processing at the edge could alleviate them and convince consumers to buy more smart products.

Hazen is designing and building a system ‘that is similar to Amazon, Alexa, Google Home or Apple Hub essentially, but it’s private by design’. This system aims at keeping all data in the home. Hazen’s project uses both federated learning (to learn from the data and update learning models) and differential privacy (to prevent possibilities of interpreting patterns)[451]. Hazen said that when he interviewed elderly people, ‘they didn’t even understand that whatever they speak goes out of their house’. Edge computing prevents their lack of knowledge to act againts them. It’s a data protection by design compliant approach, which takes vulnerable people’s needs into consideration due to its intrinsic design.

Privacy in a smart home can also mean more utility. Hazen observed that in an edge-based smart home ‘you have a holistic view of everything that happens, like your diet, your fitness, your sleep, your financial information, your activity, all of that information is consolidated inside the home’, whereas if one followed the current (cloud-based) IoT model, ‘Google needs to make sure they’re able to operate with hundreds of these apps that collect all your information outside, and they need to bring the technician outside your home’. As a result, an edge computing system could result in more utility.

Asked about data monetisation at the edge (a necessary condition for a more widespread adoption of those systems), Hazen considers that, for example, it is impossible to analyse demographics of people (which companies value) using cloud-based systems in a GDPR compliant way as this would require sending pictures to the cloud and other invasive data processes. With edge models, businesses could receive information such as gender, age and other characteristics in a privacy-preserving manner, without capturing information such as faces and other special category personal data. Hazen added that working on new ways to monetise edge-based architectural models is needed.

[451] Differential privacy means that ‘when a statistic is released, it should not give much more information about a particular individual than if that individual had not been included in the dataset’ and federated learning ‘is an emerging approach allowing the training of machine learning models on decentralised data, for privacy or practical reasons. A central server coordinates a network of nodes, each of which has training data. The nodes each train a local model, and it is that model which is shared with the central server. In other words, data is protected at the device level’. (The Royal Society 49-50 (n 7))

The analysis will now turn to challenges related to edge solutions. One of the main ones is that most companies use the cloud and all their processes are embedded into those systems. Of course, the big ones like Amazon or Google do so, but also smaller IoT companies. For example, Aland (CEO and Senior Information Regulation Officer) discussed using cloud systems as if this was the only choice a company may have. He said 'of course, we use third party infrastructure, like Amazon web servers' and he mentioned striving to make sure that the cloud systems his company uses are properly secured. There would need to be an important paradigm shift for edge computing models to take over. Of course, this is not impossible but it is a big challenge.

Beth argued that the more data goes to the cloud the more the functionality of a device can be optimised. As a repository of different persons' data, which allows to connect across different geographies, the cloud would lead to more effective products over time. According to Beth, completely abandoning cloud systems would be a negative both for the consumer and the company (in terms of optimising processes). She said that 'if you want to do one-click shopping and things like that that Amazon offers, if they don't have access to certain data of yours, it's going to be stuff that you're going to have to input every time'. She did not explain why similar data computation could not be completed at the edge in a more privacy-preserving manner. However, even if it was proven that companies can update some aspects of their smart products' more effectively using the cloud, this does not mean that sacrificing the privacy of billions of consumers would be automatically worth it.

A major problem with both cloud and edge systems has been interoperability. For example, there are devices that work with Google Home and others with Apple, but not with both companies' systems. Beth (who worked at various IoT companies) considers this as the biggest issue for smart home adoption. She has been encouraged by the development of CHIP (Connected Home over IP), a standard uniting the biggest IoT companies working on this project to ensure that devices are interoperable: 'the biggest roadblock is getting these companies to agree to work together' and she thinks first steps have now been taken in this direction.[452] Indeed, the development of this standard has been moving forward in recent

[452] Silicon Labs, 'CHIP 180 - Connected Home over IP' (2022) <https://www.silabs.com/support/training/connected-home-over-ip-intro> accessed 1 July 2022.

months. It is now called 'Matter' and, as its official website states, 'by building upon Internet Protocol (IP), Matter will enable communication across smart home devices, mobile app, and cloud services, and define a specific set of IP-based networking technologies for device certification'.[453] Its launch has been delayed until fall 2022 and its exact specificities are unknown.[454] However, companies such as Google, Amazon and Apple have all agreed to work together on making this standard a reality, which makes it a radical step to remove their technological silos. To survive and prosper, edge architectures need to be interoperable and usable with the highest number of smart devices possible. In this context, Hazen stated that currently most manufacturers design devices in such a way that they need cloud access to operate and, therefore, they cannot function with his edge computing model. A standard such as Matter could enable greater device and system interoperability, and its functionalities could be potentially integrated with edge-based architectures.

In this section, this thesis strived to show some of the merits and challenges of edge architectures mentioned by interviewees. The data protection benefits and challenges of edge-based privacy enhancing technologies (and personal information management systems in particular) will be explored in much more depth in Chapter 4 of this PhD. They could become comprehensive data management solutions to GDPR compliance and should be critically evaluated.

Section 3.6 A Summary of this Chapter's Findings

This section summarises discussions with interviewees and concludes the empirical chapter (a longer and more in-depth analysis has been provided in the previous sections). Three sub-sections give condensed answers to both research questions evaluating how GDPR compliance works in practice when vulnerable people use smart devices and how professionals perceive data protection-related issues in this context. The importance of defining, educating and guiding organisations is underlined (3.6.I), legal practical challenges are analysed (3.6.II) and technological issues and solutions are presented (3.6.III).

[453] CSA, 'Matter, The Foundation for Connected Things' (*CSA*, 2022) <https://csa-iot.org/all-solutions/matter/> accessed 1 July 2022; CSA, 'Building the Foundation and Future of the IoT' (*CSA*, 2022) <https://csa-iot.org/> accessed 1 July 2022.

[454] Jennifer Tuohy, 'Matter Smart Home Standard Delayed Until Fall 2022' (*The Verge*, 17 March 2022) <https://www.theverge.com/2022/3/17/22982166/matter-smart-home-standard-postponed-fall-2022> accessed 1 July 2022.

3.6.I Challenges Linked to the Notion of Vulnerability

Most organisations producing smart devices for the general population do not take vulnerable adults' needs and rights into consideration within their data processes and larger IoT companies sometimes even ignore children's rights even though the latter are explictly mentioned multiple times in the GDPR. There is a need of a wider discussion and conclusions regarding how to approach the notion of vulnerability in the GDPR context (similarly to the notion of fairness) in order to make it more tangible and applicable in practice by companies developing smart products, especially in relation to vulnerable adults. More awareness is required among consumers concerning data related-issues so that they can make informed choices and influence organisations by demanding GDPR compliance themselves. Moreover, sector specific guidance in the IoT sector should be published, taking into consideration vulnerable groups, as many companies are still unaware of various GDPR obligations or how to interpret them. While some smaller organisations seem to fear enforcement actions, there are also those, which consider that they will not be targetted by DPAs due to their limited size even if they make certain mistakes. This is probably due to the rather rare enforcement actions from usually underfunded DPAs. One company has self-declared violating GDPR provisions to a DPA when processing vulnerable people's data. Such choices should be promoted to resolve GDPR violations as quickly as possible. Experts consider that reflection on how to support more effective and currently unsatisfactory enforcement measures is needed. A vulnerability-aware approach could increase the data protection of all citizens as well as organisations' GDPR compliance.

3.6.II Analysing Professionals' Approach to GDPR Implementation When Vulnerable People Use Smart Devices

The doctrinal chapter analysed consent's conditions by providing examples of circumstances involving vulnerable persons using IoT devices and how businesses should adapt measures in this specific context. The business reality is that consent is portrayed as the least popular legal basis by most companies developing smart products, precisely because of those additional legal hurdles and due to the high bar of consent requirements in general. Some also consider that consent may be negative for vulnerable individuals as they might reject useful devices without making truly informed choices while others, on the contrary, underline that consent may empower data subjects and that problems are linked to how it is currently designed. In practice, performance of a contract and legitimate interests are preferred by professionals. The extent to which the latter will be beneficial for vulnerable people's rights depends on whether a company has actually gone through in-depth balancing exercises (as posited in Chapter 2 as well).

Transparency is an overarching principle that should concern all types of communications which is not always the case within IoT companies. While adapting measures to a level children can comprehend is important, there is also a real need to have materials prepared for various types of vulnerabilities, for example, for visually impaired persons. Professionals use and recommend documents in easy-read, just-in-time notices, videos and gamification as ways to improve communication mechanisms. University researchers also suggest the involvement of vulnerable individuals in the design of transparency measures.

In terms of the fairness principle, it is not applied in practice due to the lack of its comprehensive definition. Professionals need academics and courts to establish analytical frameworks in this regard. In Chapter 2, this thesis has mentioned fair balancing exercises and fair transparency as examples of how fairness could be applied by data controllers. In the empirical study, experts proposed to link fairness to other more tangible concepts such as the best interests of the child principle established in the Convention on the Rights of the Child or to human rights[455]. Fairness might need to be broken down into various parts just like data protection is a more specific notion within the concept of privacy. While fairness is context-dependent and elusive at the moment, it is a GDPR principle, which must be applied by IoT companies, especially when vulnerable people use smart devices. More guidance is needed in this context.

Companies presented vulnerable people's data collection and processing by smart devices as justified for two main reasons. Firstly, to provide support in exceptional circumstances, such as when older people are targetted for fraud-related reasons or when they have a fall. Secondly, to improve IoT products and offer increasingly effective and efficient services to their consumers. Representatives of those organisations stated that this is in the best interests of vulnerable persons. However, risks related to data overcollection are increasing. Vulnerable

[455] Convention on the Rights of the Child (n 4).

people whose personal data is collected can be used, for example, for behavioural targeting or they can become easy targets for cybercriminals. Lawyers pointed out that vulnerable people's data is often a special category of personal data and an additional legal basis will be required under Art. 9 GDPR as well as more robust security measures, in-depth DPIAs and other increased GDPR obligations. As result, it is in the company's interest to minimise data collection. Some companies choose which organisations they consider more trustworthy than others to send their customers' data to for analytical purposes (for example, universities versus businesses) but the appropriateness of such distinctions is unclear. In addition to limiting data collection, certain companies limit the time in which data on a smart product can be accessed. Data minimisation has positive implications in terms of increasing customers' trust and the ability of organisations to efficiently manage their processes.

In terms of data protection by design, professionals often link this requirement to ensuring security and limiting data collection (however, by design measures are also essential, among others, in the context of transparency as mentioned in the previous chapter). By-design measures are especially important due to the fact that they often cannot be easily changed later so any wrong choices should be avoided at all costs. Unfortunately, IoT companies are not always aware of their DPbDD obligations, confuse terminology and do not implement data protection by default in a GDPR compliant manner (such as influencing consumers' choices by presenting opt-in as the better option).

Discussions on DPIAs gave the impression of an uneven level of implementation of this requirement and uncertainty regarding the considerations that should be included into them. Most IoT companies do not conduct sufficiently comprehensive DPIAs and smaller ones might benefit from the publication of templates or guidance in this regard. Some of them use external consultancy services, which can be useful to avoid conflict of interest situations (although the unfortunate lack of requirement to publish DPIAs means that external recommendations could simply be ignored). Experts consider that DPIAs should be more holistic exercises, including concepts like fairness but also other ethical and social issues that might affect data subjects (in line with this PhD's more specific recommendation to follow the rights-based and values-oriented model proposed by Mantelero).[456] Vulnerable people themselves or their carers could

[456] Mantelero (n 330).

be included in some DPIAs, depending on their condition, the level of required technical expertise and resources of the organisation.

When they implement them, companies use a variety of mechanisms and standards to certify that that they have strong security measures in place (harmonisation in this space is needed). No such compliance tools exist in the more specific context of vulnerable people's data processing. Professionals worry that if they are required to adopt certain standards, this might lead to unnecessarily high obstacles for smaller IoT companies and reduce their competitiveness. Experts note that new standards and certifications would need to be regularly updated to reflect technological developments, be audited by trustworthy organisations and provide high levels of data protection.

3.6.III Technological Barriers and Solutions to the Legal Conundrum

Professionals underline that a multidisciplinary approach is needed, in which lawyers communicate with technologists to translate GDPR principles into the design of smart technologies. IoT companies are often not aware of their obligations in relation to vulnerable people and collaboration of technologists with lawyers is required to ensure GDPR compliant by design approaches. Within smaller organisations, data protection officer roles (necessitating extensive GDPR knowledge) are often exercised by chief technology officers, further proof how in practice technology and law are intertwined within the data protection field.

Security measures can never be perfect but they might have a dissuasive effect on cybercriminals. While professionals fear that too many security layers will make access to their customers' data more difficult, this is a GDPR requirement (Art. 32), especially important considering the often more sensitive nature of vulnerable people's data. Prioritising confidentiality over control could be viewed as a paternalistic approach, whereby vulnerable people's control is taken away from them to ensure their data's security. Nevertheless, most professionals stated that they would prioritise confidentiality, not only because it reduces GDPR compliance burdens but also because in the context of protecting vulnerable individuals, they consider it more important. Interestingly, in the context of children's rights, an expert underlined that other rights (not only data protection related) should be considered in this debate, and how prioritising confidentiality over control (or vice-versa) might affect them.

Another professional stated that the real problem is data collection and that there will never be true confidentiality or control once people's data leaves a smart home. New technological architectures are needed to address the data collection, security, confidentiality and control hurdles.

Organisations are not currently capable of effectively identifying the age and identity of vulnerable people and their legal guardians, which prevents effective GDPR compliance. Customers will not necessarily reply truthfully when inputting their age information on the device, there may be incidental users of smart products in a smart home and it is important to identify the legal guardian of a vulnerable person correctly. All of this also requires new technological choices such as privacy-preserving edge-based vision systems proposed by one company as a potential solution. The assumption in big IoT companies is that families will deal with data management of various members of the household themselves. IoT organisations do not consider themselves liable and may not be able to prevent abusive uses of smart products such as smart cameras within a home but discussions on how to resolve this issue need to take place. While they may not be able to easily solve all issues, IoT companies could choose more privacy-preserving systems within which their devices operate.

Professionals agree that edge computing offers local, more privacy-preserving opportunities for data processing. Technological improvements mean that machine learning activities can now be increasingly performed at the edge as well. Some of the benefits of edge systems are avoiding cloud-related honey pots, reduced connectivity constraints, traffic, waste, energy consumption and distance that data is travelling, resulting in financial benefits for companies and greater GDPR compliance. Keeping data within the smart home can also mean more utility, giving a safer and more holistic view of everything that happens within it. Moreover, there are tangible benefits for IoT companies in terms of building trust with their consumers. While data monetisation is usually linked to cloud technologies, there are opportunities to monetise certain types of data more effectively at the edge, such as demographics of people, which would not be possible to do in a GDPR compliant manner using cloud-based systems. However, there also challenges linked to edge-based systems, one of them being the current widespread use of the cloud and difficulties in convincing companies to change their approach. Professionals consider that the cloud offers better functionality, product development and, as a result, services to consumers although they did not explain why the same functionality and development would not work at the edge. Device interoperability is essential for the adoption of both cloud and edge-based architectural models, and new interoperability standards are currently being developed.

3.6.IV Concluding Remarks

This empirical chapter presented and analysed how GDPR compliance works in practice when vulnerable people use smart devices as well as professionals' perceptions of data protection law compliance issues in this context. It has revealed challenges, problems and interesting potential solutions. Legal compliance needs to be supported by state-of-the-art technologies and edge computing models appeared in the interviews as potentially more privacy-preserving data processing architectures in comparison to the currently widespread cloud systems. Moreover, technical issues related to the identification of the users of smart devices and data co-management (by vulnerable individuals and legal guardians), as well as legal compliance hurdles with GDPR principles, raise the question of whether edge systems along with privacy enhancing technologies could help (or hinder), and to what extent, GDPR compliance in general. There is a need of holistic models of data management, which would resolve existing problems (related to, for example, age identification or user interfaces) and reduce cloud-related data privacy risks (for example, the need to trust cloud providers and unsecure cloud repositories of data). Developing on the findings of this chapter, Chapter 4 will analyse potential technological solutions grounded in normative theoretical debates to many of the problems mentioned in this empirical study and previous parts of the thesis. This PhD will now comprehensively and critically evaluate whether the edge can support better GDPR compliance and management of data when vulnerable people use smart products.

Chapter 4: Protecting Vulnerable People's Data and Complying with the GDPR through Privacy Enhancing Technologies

One of the main goals of privacy enhancing technologies (PETs) is to enable personal data processing and provide answers to data queries without allowing third parties to gain access to the whole of the data.[457] This emerging and innovative group of technologies, together with recent and on-going alterations in wider business and policy structures, could allow remarkably greater sharing and processing of data in a more privacy-preserving and trust building way. New possibilities to explore datasets could be developed leaving behind the unacceptably high levels of risks associated with current data processing practices. This chapter evaluates how the relationship between smart home devices, personal data and vulnerable people can be reshaped through PETs, in order to better protect the latter and facilitate data protection compliance. It strives to understand how to bridge the gap between law in theory and law in practice by using PETs. Theoretical discussions are also included in this chapter, as briefly exploring debates such as property rights versus inalienable rights (in relation to how data should be defined), privacy-as-confidentiality versus privacy-as-control or cloud-based data processing versus edge-based systems are necessary preconditions to being able to suggest the most relevant practical solutions.

More specifically, this part of the thesis focusses on the benefits and issues of personal information management systems (also called personal data stores, personal data spaces, personal data vaults, personal data servers, personal data management systems etc.) while also discussing PETs more broadly when theoretical debates are relevant to all of them. The term personal information management systems (PIMS) is used throughout this chapter as this is the expression that has been adopted by the European Data Protection Supervisor (EDPS) in its documents and reports.

In the first section, PIMS are briefly defined, introduced and an explanation is given as to why they are analysed in this chapter. This section also mentions the cloud versus edge computing debate and why this thesis has decided to focus on the latter (Section 4.1). The second section discusses issues surrounding the tension between confidentiality and data control in the context

[457] The Royal Society (n 7).

of PETs and smart devices used by vulnerable persons as well as practical capabilities of edge computing PIMS to enable better GDPR compliance in terms of security and data minimisation (Section 4.2). Subsequently, this PhD examines the topic of data control in more detail. Firstly, it discusses whether data should be viewed as the subject of a property or inalienable right. The topic of how PIMS should address the issue of control when vulnerable people use smart products is then analysed. How much control over their data and other people's data should vulnerable people have? How should vulnerable people's data be managed by legal guardians? The subjects of data monetisation and legal bases adopted within the PIMS context are also debated (Section 4.3). Finally, the chapter is concluded and its main findings summarised (Section 4.4).

Section 4.1 Edge-Based PIMS as a Technical Model

PIMS and PETs in general are discussed more and more often by academics, EU institutions, think tanks and other national as well as international stakeholders as potential solutions to current data protection-related problems. They could support organisations' GDPR compliance efforts when vulnerable people use their smart home devices (4.1.I). This thesis discusses the disadvantages and benefits of edge computing PIMS versus those of cloud computing architectural models (4.1.II). Such platforms have the potential to facilitate data management and security for vulnerable data subjects (4.1.III).

4.1.I A Rising Interest in PIMS

Solove argues that the 'traditional model' of defining privacy breaches as harms to specific persons ignores the fact that some data protection issues are structural and influence not only specific individuals but society in general. Solove considers that perceiving certain privacy issues as architectural proves that protecting data implies more than protecting against particular infringements. It concerns the establishment of 'a particular social structure, one that ensures individual participation in the collection and use of personal information and responsibilities for entities that control that data'.[458] Technological structures influence such social structures. As a consequence, it is important to debate how technologies influence data protection compliance and vulnerable people's rights.

[458] Daniel J. Solove, 'Identity Theft, Privacy, and the Architecture of Vulnerability' (2003) 54(4) The Hastings Law Journal 1227, 1275.

In 'Code and Other Laws of Cyberspace', Lessig underlined how code shapes behaviour in different domains and concluded that code is law.[459] Others consider that code is produced mostly through market-driven processes and, therefore, should be viewed as regulation by the market. Finally, there are those who argue that code is a completely new mode of governance that is neither law nor regulation by the market.[460] For Cohen, architectures of control created by code should be seen as 'socially driven solutions to socially constructed problems'.[461] What Cohen propounds seems essential. Regardless of how code is interpreted, all can agree that it has an undeniable influence on how people behave in the online world and, as a result, on their privacy and data, and what they can do with it. The GDPR has several provisions the objective of which is to increase vulnerable people's data protection. However, those provisions would be ineffective without appropriate technologies that can support their implementation. For this reason, it is crucial to identify, which technologies are the most suitable for this purpose and to promote their widespread adoption. As Hildebrandt suggests, a 'possible solution to the systemic gaps in legal protection is to use technology itself to enforce legal rules'.[462] The ambient intelligence in smart home environments based on real time monitoring of data subjects requires the adoption of both legal and technology tools to counter the asymmetry of power that it creates, even more so in relation to vulnerable people.[463]

In response to difficulties in enforcing legal provisions by underfunded data protection authorities, a set of technical approaches emerged under the name of privacy enhancing technologies (PET) to allow for more responsible and effective processing of personal data, often in the context of implementing privacy by design.[464] Experts who wrote the UK Royal Society's report on privacy enhancing technologies have identified five PETs as the most promising ones in terms of their potential to foster privacy-preserving data processing, namely personal information management systems, differential privacy, homomorphic encryption, trusted execution environments and secure multi-party computation.[465] This important document has influenced the choice of this thesis to focus on PIMS. PIMS can take the form

[459] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books 1999).
[460] Julie E. Cohen, *Configuring the Networked Self* (Yale University Press 2012).
[461] Ibid.
[462] Mireille Hildebrandt and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73(3) Modern Law Review 428, 443.
[463] Hildebrandt (n 114).
[464] Diaz, Tene and Gurses (n 119).
[465] The Royal Society (n 7).

of 'physical box-sets or apps on for instance phones or tablets', which can be enhanced by various types of PETs.[466] While all of the PETs mentioned by the Royal Society report have high potential to support GDPR compliance, PIMS are particularly relevant in the context of smart homes and the processing of vulnerable people's personal data in this setting as they strive to provide security, data management solutions and opportunities for users to take decisions in relation to their data. Their features encompass most of the GDPR rights that vulnerable users can exercise. They provide vulnerable people with the opportunity to decide who they wish to trust with the data they produce.[467] As it has been discussed in Chapter 2, the current practices of IoT companies often lead to clear GDPR violations such as the lack of transparently communicated information, obscure consent mechanisms, gathering data by default instead of protecting by default, lack of strong security mechanisms, lack of DPIAs (even though they are required for vulnerable people using smart products) and undermined data minimisation through transfers of large quantities of personal data to the cloud.[468] PIMS try to address the majority of those issues. They are not just tools for more privacy-preserving data processing and do not only focus on security and enforcement like many other PETs, but take into consideration the aforementioned mechanisms from the standpoint of new privacy paradigms. In some cases, they do not seem to have resolved certain issues. For example, no discussion has been identified in the literature on how PIMS operate when other legal bases than consent are adopted by organisations. In the context of the legitimate interests legal ground, there is an inherent and worrying imbalance of power between the consumers and the data controller. Even though solutions to such problems are yet to be found, PIMS could potentially help in this endeavour. This will be further discussed later in this chapter.

Moreover, from a public policy perspective, the European Commission has recently referred to decentralised data processing in its European Strategy for Data as a way to make progress in enhancing user control and GDPR compliance.[469] This shows that there is a certain momentum at European level in favour of technologies such as PIMS that needs to be recognised. There has also been an increasing interest in PIMS from the European Data

[466] Ibid.

[467] Ibid.

[468] Lachlan Urquhart, Andy Crabtree and Tom Lodge, 'Demonstrably Doing Accountability in the Internet of Things' (2018) 27(1) International Journal of Law and Information Technology 1; Nouwens and others (n 65).

[469] Communication from the Commission to the European Parliament European Commission, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020)710 final, 'A European Strategy for Data' (*European Commission*, 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN> accessed 1 July 2022.

Protection Supervisor (EDPS), universities and scholars as they allow users to have better control over their personal data and place them at the heart of decision-making.[470] Indeed, PIMS are platforms providing 'the means and infrastructure for mediating between users and those seeking to process their data'.[471] They strive to give consumers more control over how their personal data is managed (as required by the GDPR).

Article 32 GDPR mandates the adoption of organisational and technical measures to develop more secure systems that reduce the risks to persons' rights and freedoms. The choice of the technical and organisational measures lies with the controller. The use of the word 'appropriate' signifies that the controller maintains discretion as to the measures and procedures they will implement.[472] PIMS could be an effective technology to help companies in meeting their data protection compliance needs. The objectives of PIMS can be divided into three main levels: data management, infrastructure and user interaction.[473] The infrastructure level has the important goal of protecting the integrity and confidentiality of people's personal data through state-of-the-art technologies such as encryption. Data management strives to ensure the safety and effectiveness of data control mechanisms such as consent management or communication methods about personal data processing. Finally, PIMS also allow for user interaction, that is they may enable vulnerable data subjects or their legal guardians to take significant decisions in their interaction with services providers as to how their personal data is used.[474]

The rising interest in these platforms means that they should be evaluated from all angles before their potential widespread adoption. Even though many of them are yet to be commercialised, and regardless of the forms they will ultimately take, the development of PIMS has been influencing current debates both at academic, industry and political levels. As these are nascent technologies, there is an opportunity to both promote their use and fix potential issues before

[470] EDPS, 'Opinion 9/2016 on Personal Information Management Systems' (20 October 2016) <https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en> accessed 1 July 2022; EDPS, 'Personal Information Management Systems' (6 January 2021) <https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-32020-personal-information_en> accessed 1 July 2022.

[471] Heleen Janssen and others, 'Decentralized Data Processing: Personal Data Stores and the GDPR' (2021) 10(4) International Data Privacy Law 356.

[472] Hildebrandt and Tielemans (n 276).

[473] Jacques Bus and Carolyn M.-H. Nguyen, 'Personal Data Management a Structured Discussion' in Mireille Hildebrandt, Kieron O'Hara and Michael Waidner (eds), *DigEnlight Yearbook: The Value of Personal Data* (Digital Enlightment 2013).

[474] Ibid.

major problems appear. This will be discussed in the context of how PIMS could see a shift from a cloud-based to an edge-based approach to data processing.

4.1.II The Cloud and Edge Computing Approaches

In the 1950s, the computer scientist John McCarthy developed the theory of time-sharing, a predecessor of (and similar to) the current cloud computing model.[475] During this period, computing time was very expensive and organisations were trying to find ways to use it as efficiently as possible. Smaller organisations were not able to afford a computer of their own and also desired to benefit from automation enjoyed by big companies, without spending exorbitant amounts of money. This is how 'time-sharing' a computer was invented, allowing to rent a computer's computational power without having to make an enormous investment to buy a product.[476] In the 1960s and 1970s, the concept of service bureaus permitted users to share expensive computing machines. Users possessed their own terminals that executed hosted applications. A protocol transferred information from the service bureau to the remote terminal to register requests from that terminal and then transferred it back to the service bureau, which would then send it to the relevant application.[477] Historically, the cost of 'mainframe' computers, low bandwidth, often telephony based, terminal access, and that the microprocessors that enabled the emergence of the PCs had not been invented, were all reasons for the emergence of time-sharing systems. In the 1980s, computers started to be smaller with the invention of integrated circuit large enough to accommodate whole microprocessors and with less energy requirements. The immense, water-cooled systems used to compute data were no longer necessary. The notion of shared computer became obsolete as consumers were able to buy their own machines.

Time-sharing's importance has diminished with the decrease of computers' costs. However, when more and more people became connected to the Internet and mobile Internet products became widespread, this concept returned in full force under a different name – 'cloud computing'. For what reasons? Cloud computing can be defined as 'applications delivered as services over the Internet and the hardware and systems software in the data centre that provide

[475] John Patrick Pullen, 'Where Did Cloud Computing Come From, Anyway?' (*Time*, 2015) <https://time.com/collection-post/3750915/cloud-computing-origin-story/> accessed 1 July 2022.
[476] Ibid.
[477] Ibid.

those services'.[478] The services are usually called Software as a Service (SaaS) while the data centre's software and hardware are what is referred to as cloud. The present digital age is characterised by people's reliance on cloud-based architectural models. All internet users are faced with a variety of cloud options, not accessible a decade ago.[479] These cloud offerings are presented by some authors as providing an enhanced user experience 'driven by self-service, simplification, standardization, economies of scale, and technology advancement'.[480] Many services that consumers use to download apps or store their media are hosted by cloud systems, especially in the IoT field. A mix of three fundamental concepts define the cloud's objectives: 'the first is delivering a service, such as computing or storage as a utility; the second is multiple people sharing the same computer resource, referred to as virtualisation; the third is accessing services via networking'.[481] For example, even though smartphones possess the computing power of a PC, they may have insufficient storage and cloud services can be useful in this regard. As a result, some argue that the cloud provides a better user experience. How is the cloud applicable in the PIMS context? Are the benefits that made it historically useful still the only effective solution to meet consumers' and organisations' needs?

There are various PIMS currently in development, both edge computing and cloud-based, such as midata[482], DigiMe[483], CitizenMe[484], MyDex[485], IRMA[486], OpenPDS[487], CloudLocker[488] and Solid[489] (and many others). Solid, for example, is a MIT project led by Prof Tim Berners-Lee, which 'aims to radically change the way Web applications work today, resulting in true data ownership as well as improved privacy'.[490] This particular project has decided to use cloud

[478] Michael Armbrust and others, 'Above the Clouds: A Berkeley View of Cloud Computing' (*University of California, Berkeley*, 2009) <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html> accessed 1 July 2022.

[479] Blesson Varghese and Rajkumar Buyya, 'Next Generation Cloud Computing: New Trends and Research Directions' (2018) 79(3) Future Generation Computer Systems 849.

[480] Juhnyoung Lee, 'A View Of Cloud Computing' (2013) 1(1) International Journal of Networked and Distributed Computing 2.

[481] Blesson Varghese, 'A History of the Cloud' (2019) 61(2) ITNOW 46.

[482] midata, 'My Data – Our Health' (2021) <https://www.midata.coop/en/home/> accessed 1 July 2022.

[483] digi.mi, 'What is digi.me?' (2021) <https://digi.me/what-is-digime/> accessed 1 July 2022.

[484] CitizenMe, 'Global Collaborative Intelligence with ZeroData' (2021) <https://www.citizenme.com/> accessed 1 July 2022.

[485] MyDex, 'Mydex CIC Helps Individuals and Service Providers Improve their Handling of Personal Data' (2021) <https://mydex.org/> accessed 1 July 2022

[486] IRMA, 'IRMA in Detail' (2021) <https://privacybydesign.foundation/irma-explanation/> accessed 1 July 2022.

[487] OpenPDS, 'Philosophy' (2021) <https://openpds.media.mit.edu/> accessed 1 July 2022.

[488] CloudLocker, 'CloudLocker' (2021) <https://www.cloudlocker.io/> accessed 1 July 2022

[489] Solid, 'What is Solid?' (2020) <https://inrupt.com/solid/> accessed 1 July 2022.

[490] Ibid.

infrastructures. While some of the cloud-based services have moved to adopt privacy invasive models of operation, PIMS such as Solid were created to promote more privacy-preserving data processing. In terms of data confidentiality and auditability, some authors 'believe that there are no fundamental obstacles to making a cloud-computing environment as secure as the vast majority of in-house IT environments'.[491] However, there is an alternative PIMS model in the form of edge computing. Even though Solid creators are surely well intentioned, the question remains whether the benefits of cloud-based PIMS outweigh potential risks in comparison to edge computing architectures. Concerning the three fundamental concepts, which define the cloud's objectives mentioned above, recent technological developments now also allow edge solutions to be used as computing utility or storage, to share the same computer resource with several persons (virtualisation) and access services through networking. Edge computing PIMS now have the capacity to run applications needed for consumers' smart devices to function efficiently. The edge even offers better quality of service and experience for applications that need real-time response as data does not need to travel to geographically distant cloud data centres.[492] Are cloud-based or edge-based mechanisms more effective in terms of GDPR compliance? Which of those two architectural models would increase the protection of vulnerable people's data when the latter use smart home devices?

Cloud systems run applications in a centralised manner. When using this architecture, smart devices transfer the data they generate to central servers for processing. Companies implementing centralised approaches presume that consumers do not dispute the integrity of the hosting company (and the honesty of those who work for this company) nor its capabilities in terms of protecting against acute threats such as honeypots (creating economic incentives for hackers).[493] They are most probably right in many cases and vulnerable individuals may be less aware of the risks linked to cloud processing. These systems are opposite to the workings of edge computing PIMS. Edge architectures are capable of offering similar benefits to cloud-based systems with improved privacy. It is important to note that this PhD discusses home (or user-based) edge computing and not its other forms or ways in which it could be used (for example, the edge also includes phone companies hosting small cloud instances at mobile base stations, the latter achieving low latency of edge computing but none of the privacy benefits).

[491] Armbrust and others (n 478).
[492] Blesson Varghese and others, 'Challenges and Opportunities in Edge Computing' (IEEE International Conference on Smart Cloud (SmartCloud), New York, November 2016).
[493] Nicolas Anciaux and others, 'Personal Data Management Systems: The Security and Functionality Standpoint' (2019) 80 Information Systems 13.

The user-based edge model uses local data processing instead of transferring raw data to a central node. It allows for the creation of a distributed system, where personal data processing and storage takes place at the edge of the network, instead of being centralised. Transferring data to the cloud is no longer technically necessary. In edge computing, machine learning algorithms are transferred to the data and not the data transferred to the algorithms.[494] Processing the data locally can resolve many of the data protection issues linked to cloud solutions.

Moreover, decisions made by controllers concerning security measures, the choice of hardware, in what manner data will be processed to achieve a controller's objectives or who will have access to it, are now often taken in reality by cloud providers.[495] The latter support many online services used by companies developing smart products, by providing capabilities such as data management, computing and storage options. However, organisations developing and deploying smart products will remain data controllers when they outsource data storage to a cloud service 'as long as these cloud service providers act within the boundaries of their contracts with controllers'.[496] For this reason, if any data protection-related issues arise within the cloud-based system, companies producing and deploying IoT devices could be liable for the violation of their consumers' rights. PIMS architectures minimise the amount of data that is processed to respond to particular queries in line with the data minimisation principle (Art. 5.1 (c) GDPR). Only the data required to respond to a particular problem is sent to the third party. As a result, PIMS have the potential to facilitate GDPR compliance for IoT companies and increase the protection of vulnerable people's data when they use such products. In edge computing, companies are likely to face a lower level of legal risks as their vulnerable consumers' raw data would never leave the edge device without a valid reason. Local data storage and processing seems to be the main difference and argument in favour of edge computing architectures when comparing them with cloud-based models. This will be discussed in more detail later in this chapter through specific examples involving smart devices used by vulnerable people.

Databox is one example of a system that processes data at the edge of the network. This is a prototype edge computing platform that has not been commercialised yet.[497] It is a physical

[494] Ibid.
[495] Janssen and others (n 471).
[496] W. Kuan Hon, Christopher Millard and Ian Walden, 'The Problem of 'Personal Data' in Cloud Computing: what Information is Regulated? - the Cloud of Unknowing' (2011) 1(4) International Data Privacy Law 211.
[497] Urquhart, Crabtree and Lodge (n 468).

device placed in a person's house and data gathered by smart products are transferred into this system after primary usage.[498] It can be defined 'as a protective container for personal data where data may actually be located in different geographical locations. However, the Databox will act as a virtual boundary (or as a gatekeeper) where it controls how, when, what data is shared with external parties'.[499] Databox offers methods inspired by the Human-Data Interaction (HDI) model to allow people to comprehend what kind of data is collected about them and the manner in which it is processed.[500] The system is founded on isolating the raw personal data stores from other stores devoted to presenting aggregated query results, which can be transferred to remote third parties.[501]

While there are other benefits (and potential issues) linked to edge computing systems than the local data processing aspect (they will be discussed in subsequent sections), this thesis has argued in previous chapters that ensuring the integrity and confidentiality of vulnerable people's data is a prerequisite to lawful processing and that it's protection by design and by default is crucial. This seems to be better achieved through edge computing solutions. While the security of cloud-based systems can of course be increased, this PhD argues that they cannot be as secure and GDPR compliant as an edge computing system is.

With the advent of the GDPR and the capabilities of edge computing, relying on the riskier cloud architectures is no longer desirable and justifiable (as it has been the case before the development of edge technologies). Data harvesting infrastructures render data protection compliance more difficult and lead to more risks concerning vulnerable people's data. However, cloud-based systems permit companies to access important amounts of data and resources. Because many cloud applications are user-driven, this has resulted in 'opportunities for large-scale data analytics'.[502] Switching to the edge would require disrupting current business models, which will of course lead to resistance as many organisations reap economic benefits out of centralised cloud architectures. More research is required, especially in

[498] Charith A. Perera and others, 'Valorising the IoT Databox: Creating Value for Everyone' (2016) 28(1) Trans Emerging Telecommunications Technologies 1.
[499] Ibid.
[500] Richard Mortier and others, 'Human-Data Interaction: The Human Face of the Data-Driven Society' (*arXiv:1412.6159*, 6 January 2015) <https://arxiv.org/abs/1412.6159> accessed 1 July 2022; Amir Chaudhry and others, 'Personal Data: Thinking Inside the Box' (2015) 1(1) Aarhus Series on Human Centered Computing 4.
[501] Anciaux and others (n 493).
[502] Varghese and others (n 492).

economic and social sciences areas, to evaluate new business models based on PIMS edge computing systems that could potentially replace the existing cloud-based ones. The issues related to data monetisation as well as the lack of finished and well marketed products seem to be one of the biggest hurdles in terms of edge computing adoption. Edge computing needs to be monetised, just as companies using cloud computing had to be rewarded for this technology to prosper.[503] It is necessary to reach 'a critical mass of uptake that would provide confidence to other consumers and businesses' that PIMS are worth using.[504] One way to do so would be for governments to lead by example, promote and use such products, and let companies as well as consumers learn from their experience to gain trust in the edge. Cloud systems often come to mind first when thinking about data-related solutions because of their current widespread availability and adoption. However, governments and societies should strive to do more to protect their citizens' data while companies should see edge computing as an opportunity to facilitate and improve GDPR compliance, gain trust of consumers and be first movers in an emerging field.

As briefly mentioned in Chapter 3, another potential barrier to the adoption of edge-based systems is the lack of interoperability of IoT devices and the existence of technological silos within which users are forced to operate when they buy smart products. It seems crucial to push towards device interoperability, open standards and open protocols – not only to support the adoption of PIMS architectures but also for other reasons such as environmental considerations (for example, the ability of systems to work with older technologies would solve the problem of the need to constantly replace and buy a multitude of products). If smart home devices cannot be all connected together to an edge computing PIMS, the latter will not be able to accomplish its mission of a being a true smart home hub and data management platform. The PIMS called Solid (it is cloud-based) is an example of a project that strives to achieve interoperability as 'all data in a Solid Pod is stored and accessed using standard, open, and interoperable data formats and protocols'.[505] At a larger scale, the biggest IoT companies have been working on 'Matter' (mentioned in the empirical chapter), a standard enabling the communication across

[503] Rajkumar Buyya and others, 'Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility' (2009) 25(6) Future Generation Computer Systems 599.

[504] The Royal Society (n 7); Guillaume Brochot and others, 'Study on Personal Data Stores conducted at the Cambridge University Judge Business School' (*European Commission*, 7 August 2015) < https://digital-strategy.ec.europa.eu/en/library/study-personal-data-stores-conducted-cambridge-university-judge-business-school> accessed 1 July 2022.

[505] Solid, 'Fully Interoperable Standards' (2021) <https://solidproject.org/> accessed 1 July 2022.

IoT products, apps and cloud services (to be launched in fall 2022).[506] While the exact workings of Matter are still unknown, if this standard can facilitate the integration of IoT products within edge-based architectural models through device and system interoperability, this could potentially be a radical step towards a more equitable IoT environment.

This thesis analyses edge architectures from the specific perspective of GDPR compliance and vulnerable people's data protection rights. Vulnerable individuals are rarely (if not at all) mentioned in the literature in this context. When vulnerable people use smart products within a smart home system operating at the edge of the network, can PIMS help in meeting vulnerable persons' data protection needs and companies' legal obligations?

4.1.III Taking Vulnerable People's Data Protection Needs into Consideration

Data protection by individuals, also called 'do-it-yourself' data protection, is often seen as an essential part of effective and comprehensive data protection strategies. However, as some authors suggest, the wide-spread adoption of 'do-it-yourself' data protection practices is quite unlikely.[507] For this to change, data protection would need to be a 'collective, profoundly political endeavour', which it still isn't at the moment and it is rather improbable that this will change soon.[508] For now, effectively protecting data on the internet is still a skill that few people possess. It requires knowledge of various applications and software, not accessible to every member of society. In the long-lasting discussion related to the 'digital divide', some actors have blamed 'information have-nots' and 'laggards' who lack knowledge or resources instead of focussing on the actual structural reasons for inequalities in this field.[509] Such assertions ignore the needs of those who require the most protection in a smart home context – children and vulnerable adults. One cannot blame the latter for lack of enough data protection knowledge.

In some cases, data protection is becoming an expensive product feature while in others it is only attainable to those who possess substantial information on this topic. Moreover, certain

[506] CSA, 'Matter, The Foundation for Connected Things'; CSA, 'Building the Foundation and Future of the IoT' (n 453); Tuohy (n 454).

[507] Tobias Matzner and others, 'Do-It-Yourself Data Protection - Empowerment or Burden?' in Serge Gutwirth, Leenes Ronald and Paul De Hert (eds), *Data Protection on the Move Law, Governance and Technology Series*, vol 24 (Springer, Dordrecht 2016).

[508] Ibid.

[509] Ibid.

groups (for example, due to their old age or being a child) face the risk of discrimination or social stigma and, therefore, their data protection needs deserve more attention than those of other citizens.[510] Privacy should not turn into a luxury accessible to a minority of people. Individuals can only do so much to protect their data. Barriers to comprehending consequences of how their data is shared and what the users' actual choices are often prevent them from making informed decisions. Solove considers that self-management of privacy does not give individuals meaningful control over their personal data, one of the problems being severe cognitive issues (lack of knowledge and skewed decision-making) that compromise privacy self-management.[511] Those issues diminish people's capacity to make informed decisions related to the risks and potential benefits of consenting to the processing of their data, and could be exacerbated in the context of some vulnerable individuals. Furthermore, according to Solove, even well-informed persons cannot effectively self-manage their data as 'there are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity'.[512]

However, this does not mean that self-management must be completely abandoned. Instead, it should be done in a way that both empowers individuals and protects them at the same time while facilitating legal compliance. There is an inherent tension between paternalism and self-management that this thesis explores in the specific context of vulnerable people. It discusses how PETs such as PIMS can potentially become not only useful but also necessary technologies to create more just and equal societies, taking vulnerable people's data protection needs into consideration and helping them with data management. They equip consumers with a device the objective of which is to support them in controlling and protecting their data.[513] This device needs to be paid for in the first place, which creates another potential barrier. However, ensuring that the price is attainable for the average citizen would signify that a one-time payment could allow consumers to manage all of their smart home data in a safer manner on one product instead of needing to think about each IoT device separately. This is also assuming that those smart devices would be compatible with the PIMS that the vulnerable individual possesses.

[510] Ibid.
[511] Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' 1880 (n 120).
[512] Ibid.
[513] Janssen and others (n 471).

As mentioned previously, edge computing PIMS are nascent and in development. There are still many issues that need to be discussed and resolved. While PIMS have the potential of facilitating the exercise of data subjects' rights, they could also unnecessarily complicate GDPR compliance and some data management aspects for vulnerable data subjects and their legal guardians. This chapter evaluates both their benefits and potential problems when it comes to the specific case study of vulnerable people's data protection within smart homes. Theoretical debates (for example, the next section's control versus confidentiality debate), which need to precede practical considerations in order to better situate and present this PhD's arguments are also discussed.

Section 4.2 Beyond Confidentiality: The Underlying Value Orientation of PETs

This section discusses the debate on privacy-as-confidentiality versus privacy-as-control. It assesses whether confidentiality should be prioritised over control (or vice versa) in a situation where both cannot be satisfactorily achieved at the same time. This debate is applicable to all kinds of PETs, including PIMS. How should companies using PETs respond to the need of ensuring both confidentiality and control as mandated by the regulation? (4.2.I). A potential practical solution is offered through edge computing PIMS and the latter's impact on the confidentiality of vulnerable people's data in a smart home context is analysed. The practical security benefits of edge computing PIMS are explored (4.2.II) as well as how they support data minimisation (4.2.III).

4.2.I The Privacy-as-Confidentiality versus Privacy-as-Control Debate

The currently prevalent model adopted by privacy enhancing technologies of privacy-as-confidentiality (as opposed to privacy-as-control) is analysed (4.2.I.A) as well as the case study of Apple's Siri voice assistant to illustrate this PhD's position (4.2.I.B).

4.2.I.A The Current Focus on the PET Confidentiality Paradigm when Designing IoT Products

Privacy by design obligates manufacturers of IoT devices to embed data protection from initial design stages.[514] Data protection principles should be implemented 'directly into the design specifications of the technological systems', in order to incorporate privacy considerations in the functioning and management of data processing.[515] Privacy by design also supports the regulation of data subjects' rights and narrows the legal shortcomings resulting from slow adaptation of legislation to fast technological developments.[516] Bringing data protection laws to life is to a large extent reliant on software design, and the latter is the outcome of experts' inclinations and decisions or, in the worst-case scenario, their lack of understanding and concern to protect personal data.[517]

Gürses drew attention to the techno-centric nature of data protection and the focus on data confidentiality adopted by many computer scientists.[518] Techno-centricity can be defined as an interest 'in understanding how technology leverages human action, taking a largely functional or instrumental approach that tends to assume unproblematically that technology is largely exogenous, homogenous, predictable, and stable, performing as intended and designed across time and place'.[519] It focusses on the effects of the technology while ignoring how it is linked to historical, cultural and social influences. This approach is opposite to human-centricity, which places the way in which people make sense of and use technology at the forefront. Human-centric approaches seem to reflect GDPR's focus on control (in addition to confidentiality) and its differentiation between vulnerable and other citizens. Human-centricity does take social, cultural and historical contexts into account but tends to minimise the role of technologies.[520] As Gürses has stated, 'social practices in spaces subject to ubiquitous surveillance are constituted by existing surveillance practices, technologies and by PETs, whereas PETs are the product of humans, their own social practices and conceptions of how surveillance is made effective and can be countered'.[521] When thinking about data protection by design, neither the confidentiality techno-centric nor the control human-centric approaches

[514] Article 29 Working Party, 'Opinion 02/2013 on Apps on Smart Devices' (n 264).
[515] Anna Romanou, 'The Necessity of the Implementation of Privacy by Design in Sectors where Data Protection Concerns Arise' (2018) 34(1) Computer Law & Security Review 99.
[516] Urquhart (n 273).
[517] Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24(2) International Journal of Law and Information Technology 151.
[518] Seda Gürses, 'PETs and their Users: a Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm' (2010) 3(3) Identity in the Information Society 539.
[519] Wanda J. Orlikowski, 'Sociomaterial Practices: Exploring Technology at Work' (2007) 28(9) Organization Studies 1435.
[520] Ibid.
[521] Gürses.

seem sufficient. Both should be combined together. Technologies could achieve much more if they include social and other contexts into their development processes (reflecting GDPR's requirement to take special data protection measures in relation to vulnerable individuals). Ultimately, their role should be to be inclusive of all those considerations if they are not to be perceived as a tool for elites to implement their vision of progress. Before delving deeper into this topic and analysing the control and confidentiality entanglement, it is necessary to respond to the question as to what this thesis means by privacy-as-confidentiality and privacy-as-control.

Privacy-as-confidentiality strives to ensure that technologies support minimal information loss or leaks from persons using smart products. This is distinctive of PETs, whose researchers use mainly cryptographic methods to, for example, perform analysis on whole datasets while learning as little as possible about the persons within them.[522] Privacy-as-confidentiality is characterised by an environment full of adversaries who cannot be trusted. PET researchers often consider that the main objective of privacy technologies is to respond to risks associated with untrusted environments. Privacy-as-control, on the other hand, tries to build trust between organisations that could otherwise be considered as adversaries, and turn them into 'responsible stewards, rather than ruthless exploiters, of data'.[523] It is the GDPR's approach, through which the regulation mandates data controllers to respect the rights of data subjects, such as the right of access or erasure of their data.

Some authors consider that trade-offs between control and confidentiality intrinsically underpin certain data subject rights such as data access request verification procedures.[524] The 'linkability' between the data subjects making data access requests and their persistent identifiers illustrates this intrinsic tension.[525] Privacy enhancing processes that weaken the link between the data subjects and their data (for example, pseudonymised persistent identifiers) reinforce confidentiality. Inversely, a strong link between the data subject and their identifier diminishes confidentiality but increases control as data access processes are made easier. The

[522] Vasilios Mavroudis and Michael Veale, 'Eavesdropping Whilst You're Shopping: Balancing Personalisation and Privacy in Connected Retail Spaces' (Proceedings of Living in the Internet of Things: Cybersecurity of the IoT, London, 2018).
[523] Ibid.
[524] Rebecca Iafrati, 'Can the CCPA Access Right Be Saved? Realigning Incentives in Access Request Verification' (2020) 20(1) Pittsburgh Journal of Technology Law & Policy.
[525] Ibid.

GDPR mandates access request verification but does not explain what this verification should consist of. This suggests that operationalising a verification procedure that adequately balances control and confidentiality is not an easy task. Facilitating access rights while not decreasing the security of personal data is difficult.[526] According to some, 'privacy is no longer a case of Pareto improvement (under which it can masquerade as a unified concept), but requires choosing a certain approach (e.g. confidentiality) to the detriment of others (e.g. control)'.[527] They argue that there are trade-offs that organisations must engage with, otherwise outcomes will be determined randomly.[528]

Even though legislation now uses the more precise notion of data protection by design (as opposed to the more fluid notion of privacy by design), and even if regulatory guidance and legal scholarship have underlined the wide variety of objectives that data protection by design should strive to achieve, the latter is frequently constricted to the PETs model of privacy-as-confidentiality. Some researchers criticise this focus of PETs on the prevention of information disclosure instead of ensuring the protection of all data protection principles and GDPR rights.[529] They flag the emphasis of PETs on privacy-as-confidentiality as opposed to privacy-as-control (GDPR's approach) and underline that data protection by design requires controllers not only to implement confidentiality-related mechanisms but also to enable data subjects to exercise their rights (such as the right to erasure, right of access, portability or right to object) and to promote controllability, data minimisation, user friendly systems, transparency and other GDPR provisions.[530] While PETs cannot always prevent data protection breaches (there will always be capable adversaries), they can minimise risks. However, they often do so at the expense of the possibility to exercise other data subjects' rights. This can impede data subjects' ability to manage data risks themselves. In the context of smart devices used by vulnerable people, is achieving confidentiality more important than promoting control? What kind of data protection-related trade-offs (if they are really needed) should be made to support organisations' GDPR compliance and the protection of vulnerable data subjects' rights? There are data controllers who follow an interpretation of the GDPR that makes it more difficult to

[526] Ibid.
[527] Veale, Binns and Ausloos (n 117).
[528] Ibid.
[529] Ibid.
[530] Article 29 Working Party, 'The Future of Privacy. Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data' (WP 168, 2009).

exercise certain data protection rights. They make design choices that lead to this outcome. Should they change their approach? To provide an answer to this question, this thesis will now discuss Apple's voice assistant Siri as an example.

4.2.I.B Investigating Privacy-as-Confidentiality through Apple's Siri Voice Assistant

Voice assistants are increasingly popular in smart homes and they will be used more and more often by vulnerable people. How are data protection considerations included into their design? In particular, how does Apple include those considerations into its Siri voice assistant? Companies sometimes agree to provide data recorded by a voice assistant to the data subject under the right of access (Art. 15 GDPR). For example, Google provides a mechanism through which the data subject can manage voice and audio data that has been recorded by Google's audio assistant. However, not all organisations do this. There is research in the literature highlighting this topic. After an explicit request to obtain personal data recorded by Apple's Siri voice assistant, the company declined justifying this by the notion of privacy by design.[531] Firstly, Apple stated that data linked to a voice identifier is separated from other identifiers. Device-specific identifiers are disassociated from other types of identifiers used by the company. Apple informed that they do not possess technical capabilities to obtain the voice assistant's identifier or to search data associated with it as they have not built a system permitting them to do so. Apple also asserted that links between identifiers and data gathered by Siri are generally deleted and that this data is eventually erased after specific periods of time. Finally, the company maintained that even if Siri is capable of identifying a data subject's name when they use its services, this capacity is only enabled by the transfer of relevant data each time the voice assistant is activated (and not by storing this data permanently). If Siri is not activated for more than ten minutes, this personal data is erased from Apple's servers.[532] Veale et al have criticised Apple's approach. Among other arguments, they consider that the decision not to create a database retrieval tool does not justify refusing data subjects' rights and that declining to make it possible to obtain the device identifier does not seem to have any valid reason in practice other than limiting the exercise of those rights.[533] Apple's decisions are an example of embedding privacy into data management and software that has focussed on what other authors described as a 'rather narrow definition of privacy, which largely addresses

[531] Veale, Binns and Ausloos (n 117).
[532] Ibid.
[533] Ibid.

confidentiality and data security'.[534] While Apple has adopted this approach, which certainly has its flaws and could be improved, how can their confidentiality-focussed privacy by design choices be evaluated in the context of a vulnerable person using Siri?

It is important for a company to explicitly state why it gives priority to data confidentiality over other GDPR rights that data subjects should normally be able to exercise. It is reasonable to expect Apple to explicitly justify that approach. It is not acceptable to simply affirm (what governments sometimes do), without any real arguments, that rights are part of a 'zero-sum game along with collective security', and that the only manner to foster the latter is to limit the former.[535] Similarly, it is not acceptable (what companies often do) to only think about rights as risks to the company and, therefore, to limit the exercise of those rights to avoid further risks or court cases.[536] It is uncertain what has been Apple's true rationale for limiting data subjects' rights and this should have been explained. Rights and freedoms of the data subject need to be safeguarded (Art. 35 GDPR). Having said that, in some situations, limiting a data subject's rights could be an adequate solution if transparently explained, for example, through the publication of a data protection impact assessment. From the perspective of a vulnerable person's needs and considering GDPR's provisions on the necessity to adopt special protection measures in relation to children (Rec. 38 GDPR) and to tackle increased risks when vulnerable people's data is processed (Rec. 75 GDPR), Apple's approach of insisting on confidentiality over the possibility of exercising other data subjects' rights could be correct. Of course, if confidentiality and the exercise of other rights can both be achieved at a satisfactory level, then it should be done so. In any case, efforts should be made in this direction. While waiting for the adoption of such systems (which should be promoted and researched), this thesis considers that the confidentiality of a vulnerable person's data should be the top priority. If there can be people able to effectively manage and protect their personal data, for children or some adults with cognitive disabilities the benefits of being able to exercise their right of access (for example) will probably not surpass the benefits of higher data confidentiality (if exercising this right would result in the creation of higher data breach risks). Again, this should be a transparent balancing exercise performed by data controllers through an evaluation of the technologies at their disposal as well as by courts and regulators to guide data controllers in their decision-making. Organisations could do this through data protection impact assessments

[534] Wiese Schartum (n 517).
[535] Van Dijk, Gellert and Rommetveit (n 317).
[536] Ibid.

the results of which would ideally be published (unfortunately, there is no legal obligation to publish DPIAs in the GDPR). In such impact assessments, fundamental rights and freedoms of vulnerable individuals should be taken into consideration alongside GDPR provisions, in line with the spirit and provisions of the regulation. Giving priority to confidentiality in data protection by design approaches should not be the approach by default but the result of an in-depth analysis of what is the overall best solution for data subjects' protection of data and fundamental rights. Data controllers should regularly re-evaluate their approach in line with the 'state of the art' criteria that requires them to stay up to date with technological developments and how the latter can support the implementation of GDPR's provisions.[537]

It is worth mentioning that the data controller is not 'obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation' (Art. 11 and Rec. 57 GDPR). This might be interpreted as meaning that the GDPR itself has implied the confidentiality over control approach should prevail in certain scenarios. As a result, in the Siri case study, Apple is not obliged to allow for the exercise of certain data subjects' rights if it can demonstrate that it is not possible for the company to determine a data subject's identity. However, the data subject can provide additional information to Apple to enable such identification voluntarily (this is mandated by the GDPR in the same article). This provision could allow ordinary citizens to exercise their data protection rights even though this has been made more difficult by Apple's privacy by design measures, while allowing for vulnerable people's data to be hopefully better protected. In any case, Apple should explain why it gives priority to confidentiality over other rights and how ordinary citizens can exercise those rights if they want to. It should be transparent about its processes.

The findings of this section on the privacy-as-confidentiality versus privacy-as-control debate apply to PIMS and all other PETs. Confidentiality means that someone is excluded from the observation of others while control is a model enabling the data subject. Theoretically, these two values of confidentiality and control do not need to be mutually exclusive. As Cohen has stated back in 2000, 'the characterization of the data privacy problem as driven by technological trade-offs grossly oversimplifies the choices that we face' because 'architectures

[537] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (n 173).

of data collection are chosen'.[538] And what is chosen can be changed. There is a possibility that an instrument could serve both purposes. Edge computing PIMS presents an opportunity to explore such a solution. Indeed, Apple seems to be moving further into the edge computing direction with Siri. The recent iOS 15 update in June 2022 allows to use a Beta version of Offline Siri (the full release is predicted 'in the fall') resulting in enhanced privacy due to the speech recognition tasks being performed on-device and the speech data not leaving the iPhone (the benefits of edge-based processing are explored in more detail below).[539]

Some have argued that to ensure effective protection against risks associated with data controllers, privacy enhancing technologies need to combine three principles: 'elimination of the single point of failure inherent with any centralized trusted party; data minimization; and subjecting protocols and software to community-based public scrutiny'.[540] This can be achieved through edge architectures. The latter's objective is to ensure that data's confidentiality is protected (especially through local data storage) and, at the same time, that consumers can exercise control over their data. The security and control-related benefits and issues of using PIMS by vulnerable individuals in smart homes will be discussed in the next sections.

4.2.II The Security Benefits of Local Data Storage

Processing vulnerable people's data at the edge of the network increases its security (4.2.II.A). The example of smart toys shows how PIMS' characteristics can help in actively resolving several security issues currently linked to many smart devices used by vulnerable individuals (4.2.II.B). Edge computing PIMS also increase vulnerable persons' data security through their capabilities combined with apps that can be installed on those systems (4.2.II.C).

4.2.II.A Increasing Security by Processing Data at the Edge of the Network

The insecurity of smart homes is currently an important problem in the world and many essential security features are missing in smart devices (such as regular software updates or

[538] Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' 1436 (n 274).
[539] Sanuj, 'iOS 15: How to Use Siri Offline on iPhone and iPad (Without Internet)' (*iGEEKSBLOG*, 9 June 2022) <https://www.igeeksblog.com/how-to-use-siri-offline-on-iphone-ipad/> accessed 1 July 2022.
[540] Diaz, Tene and Gurses 940 (n 119).

strong authentication measures).[541] Moreover, most IoT devices transfer users' data to the cloud, either for computation or storage. As it has been mentioned already, protecting the integrity and confidentiality of vulnerable individuals' personal data should be the top priority. The cloud does not ensure this. PIMS based on cloud infrastructures could expose users to a range of risks. Firstly, unauthorised access by some of the cloud provider's personnel may still occur despite strong security measures in place. Secondly, the personal cloud code would need to be completely trustworthy, which is not possible as any application or service offered on the internet can be hacked. Such applications or services are valuable targets for cybercriminals as cloud infrastructures usually contain data of many users. Data breaches 'resulting from attacks conducted against the personal cloud provider or the applications (which could be granted access to large subsets of raw personal data), or resulting from human errors, negligence or corruption of personal cloud employees and application developers, cannot be avoided in practice'.[542]

For this reason, this thesis argues in favour of recognising the value of local data processing and edge computing architectures, especially in light of the importance of the integrity and confidentiality of vulnerable people's personal data. Edge computing models are emerging in some degree as a response to the increased number of insecure smart devices and the associated growing amount of data collected by companies for data analysis purposes. In edge computing, the physical infrastructure that hosts computing resources is placed 'in close geographical proximity to where data are generated or needed for processing'.[543] This approach has advantages in terms of facilitating data protection compliance and security management in people's homes.[544] While simple storage of encrypted data as backup in the cloud may not create substantial data security risks (password managers are a good example), moving the point of computation to the end-device reduces the number of places where data needs to be made available unencrypted. Databox is an example of a PIMS that carries out data computation

[541] Kayleen Manwaring, 'Emerging Information Technologies: Challenges for Consumers' (2017) 17(2) Oxford University Commonwealth Law Journal 265; Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World* (Norton 2018); Scott R. Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' (2014) 93(1) Texas Law Review 85.

[542] Anciaux and others (n 493).

[543] UK Parliament, 'Edge Computing, Postnote 631' (2020) <https://post.parliament.uk/research-briefings/post-pn-0631/> accessed 1 July 2022.

[544] EDPS, 'Opinion 9/2016 on Personal Information Management Systems' (n 470); Jiahong Chen and Lachlan Urquhart, 'On the Principle of Accountability: Challenges for Smart Homes and Cybersecurity' in Andy Crabtree, Haddadi Hamed and Mortier Richard (eds), *Privacy by Design for the Internet of Things: Building Accountability and Security* (IET 2021).

locally. This prevents inherent security risks of data processing in the cloud. Apple has been also introducing more edge-based data processing solutions through its HomeKit System. The HomeKit Secure Video analyses security footage gathered by IoT products at the edge, within people's homes.[545] Subsequently, only encrypted results of this processing are sent into the cloud. Companies need to ensure that vulnerable people's data is processed by IoT devices in a secure manner and processing this data at the edge would support their compliance efforts with GDPR's integrity and confidentiality principle, a prerequisite for lawful data processing.[546]

In addition, another security benefit in the context of edge computing architectures is that actuation does not depend on uninterrupted connection to the internet, which increases the system's resilience and reduces data processing costs.[547] While those benefits may not seem directly related to data protection compliance in the context of smart devices used by vulnerable individuals, in reality they are. For example, a hacker might deprive the smart home of its internet connection for criminal purposes. If vulnerable adults are the targets, they might be in greater danger than ordinary citizens. If their smart lock stops functioning due to interrupted connectivity this could lead to more distress than for ordinary citizens. Computation at the network's edge would prevent this from happening.

In the absence of sufficient security features in IoT devices and in the context of security issues linked to processing data in the cloud, edge computing PIMS could help data controllers in their compliance efforts and vulnerable people in protecting their data. This thesis will now discuss this through the examples of smart toys.

4.2.II.B The Example of the Hello Barbie Doll Smart Toy

In 2015, Mattel produced a smart device called the Hello Barbie doll. This Wi-Fi enabled smart toy was presented as the first interactive doll ever created, capable of listening and having conversations with children. The doll has a microphone which records children and then sends those recordings to third parties for data processing. Matt Jakubowski, a security researcher working in the field of cybersecurity, was successful in quickly hacking the doll. This allowed

[545] Jakub Lewkowicz, 'Apple shows off new security features, iOS 13 and new iPad OS at WWDC' (*SD Times*, 3 June 2019) <https://sdtimes.com/softwaredev/apple-shows-off-new-security-features-ios-13-and-new-ipad-os-at-wwdc/> accessed 1 July 2022.

[546] GDPR, art 5 (f).

[547] Crabtree and others (n 165).

him to access the system, acquire account data, files containing audio recordings and to use the toy's microphone itself.[548] Children could be the target of hackers for various reasons. They could be used to acquire sensitive information or their toy could be hacked to gain access into other smart devices in the smart home. There are substantial amounts of money spent on the marketing of such smart toys. They are therefore visible targets for cybercriminals.

The Hello Barbie doll is of course not the only smart home toy presenting important security issues. Cayla, for example, is another doll that has been criticised by German authorities as it enabled spying on smart home members and acquiring their personal data.[549] Cayla then sent the data it gathered to the United States. This not only endangered the targeted family but also was not compliant with GDPR's provisions, such as those concerning limitations of personal data transfers to third countries. In addition, a technical analysis commissioned by the Norwegian Consumer Council revealed that any person could gain access to the microphone and speakers of Cayla.[550] Physical access to the doll was not needed. This important security defect was the consequence of the absence of any security measures related to the doll's Bluetooth connection. Any person within 15-meters of Cayla would have been capable to connect to the device and use this connection for criminal purposes.

In both cases, the dangers concerning data transfers into the cloud for processing by unknown third parties could be reduced by using edge computing PIMS. For example, the edge computing Databox system 'enables the data subject to control external access to data via app manifests that provide granular choice encoded as enforceable data processing policies on-the-box, and constrains data distribution to the results of processing'.[551] In addition, 'The IoT Databox stores data in a distributed array of containers, which encrypt data at rest'.[552] With this kind of architecture present, the hacker would need to surpass those security features to gain access to the smart toy's data. Children's voices would not be transferred to the cloud but stored locally. Unusual activities of the smart toys would be detected, parents would learn about this

[548] Gibbs (n 340).
[549] Amanda Erickson, 'This Pretty Blond Doll Could be Spying on your Family' (2017) <https://www.washingtonpost.com/news/worldviews/wp/2017/02/23/this-pretty-blond-doll-could-be-spying-on-your-family/?noredirect=on&utm_term=.00adeafac872> accessed 1 July 2022.
[550] Forbrukerradet (Norwegian Consumer Council) (n 341); Bouvet on behalf of the Norwegian Consumer Council (n 341).
[551] Urquhart, Crabtree and Lodge (n 468).
[552] Ibid.

thanks to the Databox interface and would be able to stop data from leaving the box (as their consent for any unusual data processing would be required).[553]

4.2.II.C Protecting Vulnerable Adults through Apps Installed on PIMS

PIMS may enable consumers to use their data for personal benefit for various purposes, one of them being improved security.[554] How can this be achieved? Vulnerable adults, such as people living with dementia, are unfortunately often deceived by criminals into giving sensitive information about their bank accounts or to transfer money in promise of receiving something valuable in return. These stories regularly appear in the media and resolving this problem would have an important societal value.[555] Cybercriminals might hack into a smart device and obtain personal data themselves or contact their target through a smart product. Databox, for example, could help in such circumstances by detecting unusual activities and informing the relevant person or institution. The Databox enables its owner to install apps on its system. A vulnerable adult or the legal guardian could download a bank's fraud detection app. The bank would contact the app in case of unusual activity. The user's precise location would not be disclosed but only information on whether they are located where the unusual activity is taking place.[556] The bank would then be able to prevent fraud and protect vulnerable individuals, the most frequent victims of these kinds of criminal activities. All of this would happen in a privacy-preserving way in which only the data necessary to answer a particular query (is the data subject located where the unusual activity is taking place?) would be transferred to the third party asking for information. Such an app can be installed on the PIMS and integrated with all of the data traffic coming from vulnerable people's smart devices.

4.2.III Minimising Data Processing Risks by Answering Only Specific Queries

PIMS reduce risks related to data transfers by minimising the amount of personal data transferred to third parties for processing (4.2.III.A). They can support more privacy-friendly mechanisms related to obtaining users' age and consent from their legal guardians (4.2.III.B).

[553] Crabtree and others (n 165).

[554] Alan Chamberlain and others, 'Special Theme on Privacy and the Internet of Things' (2018) 22(2) Pers Ubiquit Comput 289.

[555] Financial Times, 'Living with the Cost of Dementia' (2021) <https://www.ft.com/content/4baeeb4e-d680-11e6-944b-e7eb37a6aa8e> accessed 1 July 2022.

[556] Chamberlain and others (n 554).

4.2.III.A The Reduction of Risks Related to Data Transfers

PIMS can help in satisfying the requirements of the data minimisation principle (Art. 5.1 (c) GDPR). As mentioned previously, certain PIMS take 'computing to the data, rather than data to the computing as per the current 'cloud' paradigm, and this has distinct computational as well as social advantages'.[557] Firstly, this removes the necessity for international data transfers to remote servers in third countries, which are far from being automatically allowed by the GDPR (as the CJEU has also explicitly affirmed in several cases, the most well-known being the *Schrems* judgments).[558] The need for such transfers would make compliance more difficult for companies producing smart devices. Indeed, the level of data protection provided in third countries is not always considered sufficient and once data is sent abroad, it may be more difficult to control who gains access to it and where the data points are stored.[559] Local data storage could be a more effective solution for companies (less compliance problems), vulnerable consumers (more secure and safer data processing) and the smart home market overall (increased trust of consumers as a result of increased data protection). If data processing is done locally rather than in the cloud through centralised storage and computation, this would reduce data processing and, therefore, increase compliance with the data minimisation principle.[560]

Some authors explain that in line with the data minimisation principle smart devices should reduce the amount of data transferred from smart products by changing raw data into aggregated data and deleting the former as soon as the data necessary for processing has left the device.[561] This is exactly what edge computing architectures strive to achieve. Only the required data to reply to a particular problem or query is transferred to third parties. Moreover, developments in federated learning signify that it is conceivable for distributed data analytics to be done in manners that are more privacy-preserving.[562] Contrary to the usual machine

[557] Ibid.

[558] Maximillian Schrems v Data Protection Commissioner (Schrems), Case C-362/14, [2015] (ECLI:EU:C:2015:650); Facebook Ireland Ltd vs Maximillian Schrems (Schrems 2), Case C-311/18, [2020] (ECLI:EU:C:2020:559).

[559] Urquhart, Crabtree and Lodge (n 468).

[560] Crabtree and others (n 165).

[561] Ibid.

[562] Carmela Troncoso and others, 'Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments' (2017) 4 Proceedings on Privacy Enhancing Technologies, De Gruyter Open 307.

learning model based on centralised approaches, 'federated learning is a decentralized training approach', which allows products 'located at different geographical locations to collaboratively learn a machine learning model while keeping all the personal data that may contain private information on the device'.[563] This approach is more compatible with the requirements of the GDPR Article 5 data minimisation principle.

4.2.III.B Minimising Data Collection when Obtaining Information on Users' Age or Consent from their Legal Guardian

As it has been discussed in the doctrinal chapter, there are on-going discussions on how service providers should meet the requirement to obtain information about the age of their users, and how they will make sure that parents have really consented to their children's data being processed (or legal guardians in the context of vulnerable adults).[564] Even though there is no explicit provision in the GDPR that mandates data controllers to ask about data subjects' age, this is still necessary as processing on the basis of consent obtained from an underage child would be unlawful. This needs to be done in conformity with the data minimisation principle, enshrined in Art. 5.1 (c) GDPR. One benefit of PIMS in this context is that all smart home devices would receive the relevant information (about the legal guardian or data subject's age) from the PIMS, without the necessity for each device to ask the same questions. Moreover, this information would be collected at the edge, without the need to worry about excessive data collection by data controllers. Only the required information (confirmed age or identity) would be transferred to the relevant third party.

In terms of how this could be achieved, this is more of a question of how to do it effectively and in a privacy-preserving manner, as in terms of security, vulnerable people's data would be kept on the PIMS itself. However, this is also crucial for vulnerable people's data protection rights. If the identification of a vulnerable person or their legal guardian is made difficult, they will not be able to easily exercise their rights in a safe manner. Firstly, PIMS would need to be able to contain information on who is a person's legal guardian or who is a child's parent. To obtain such information, the PIMS could, for example, make a request to a governmental

[563] Zengpeng Li, Vishal Sharma and Saraju P. Mohanty, 'Preserving Data Privacy via Federated Learning: Challenges and Solutions' (2020) 9(3) Ieee Consum Electr M 8.
[564] Milkaite and Lievens, 'The Internet of Toys: Playing Games with Children's Data?' (n 440).

database. However, this request should not divulge unnecessary data to third parties and only information that a request has been made should be transferred.

In certain cases, data subject's identification could be also facilitated through the use of biometrics. However, in Europe, biometrics seem to be often associated by citizens with privacy invasive technologies. This could be changing (or not) with the appearance of new phones and other devices using such means to identify their owners. If the costs are not prohibitive and biometric identification can be done on the edge, in a privacy-friendly way, then it could be a more effective solution. For example, facial recognition could recognise whether the user is a child. This would facilitate further actions within the PIMS as the system would know that the user is underage. In the case of children, biometrics would have the added benefit of simplifying the process as connecting to a database to confirm whether the user's response is correct would no longer be necessary. Of course, data controllers could just trust data subjects' responses without further verification but it would be naïve to think that those responses would always be truthful.

Section 4.3 Property or Inalienable Rights? The Legal Paradigms of Controlling Data

This thesis examines the concept of data ownership and whether people can irreversibly separate themselves from their personal data, discussing arguments both in favour and against treating personal data as property rights while ultimately arguing in favour of the latter (4.3.I). Subsequently, it discusses how vulnerable people's data should be managed when collected by smart home devices and reflects on how PIMS can support GDPR compliance in this context (4.3.II).

4.3.I The GDPR Fundamental Rights Approach versus Personal Data as a Property Right

Should one's control over their own data be viewed as property or inalienable right? Firstly, different approaches as to how control and ownership of personal data can be viewed are introduced (4.3.I.A). Secondly, arguments in favour of data ownership are briefly discussed (4.3.I.B) before making an even stronger case in favour of limiting individuals' control over their personal data and against considering data as property (4.3.I.C).

4.3.I.A Introducing Different Approaches to the Control and Ownership of Personal Data

Data protection is viewed differently depending on the country and geographical region. There are some people who advocate the existence of full data ownership by data subjects[565] and the monetization of access to a person's data through transfers of its ownership.[566] According to this approach, once data is sold to another party, the latter would have full ownership of the data, meaning that they can resell the data without the permission of the individual, and the individual does not have the right to unilaterally withdraw from that arrangement. As a result, individuals could completely lose control over personal data and be unable to change this. There seems to be a cultural difference whereby this property approach is more popular in countries such as the United States where the standards of data protection are often very different from those in the European Union, as has been established in CJEU *Schrems* cases.[567] In many States, limited sector specific data protection provisions still exist and data there is frequently considered as property for which data subjects should be compensated.[568] Contrary to the United States and some other countries, the majority of current legal systems do not confer proprietary rights in data.[569] In the EU, protection of personal data is more often viewed as a fundamental right, which the data subject cannot be irrevocably separated from.[570] EU advocates of individual control over data protection are suspicious of the market-based approach to personal data which property rights would bring.[571] Notwithstanding the use of the term ownership often heard in data protection debates, 'the EU data protection regime, at best, enables individuals to exercise rights akin to licensing rights over their personal data'.[572] The difference between EU data protection provisions and regimes such as the United States one is

[565] Leonard J. Kish and Eric J. Topol, 'Unpatients - Why Patients Should Own their Medical Data' (2015) 33(9) Nature Biotechnology 921.

[566] Mark A. Hall, 'Property, Privacy and the Pursuit of Integrated Electronic Medical Records' (2014) ssrn: 1334963 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1334963> accessed 1 July 2022.

[567] *Schrems* (n 558); *Schrems 2* (n 558).

[568] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2018) 22(2) Pers Ubiquit Comput 317.

[569] Osborne Clarke, 'Consumer Data and the Complex World of Data Ownership' (2015) <https://www.osborneclarke.com/insights/consumer-data-and-the-complex-world-of-data-ownership/> accessed 1 July 2022.

[570] Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20(6) German Law Journal 779.

[571] Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 231.

[572] Ibid 230.

that the former limits data subjects' individual control over their data whereas the latter may allow full control.

In civil law countries, ownership of personal data would mean 'full-ownership, i.e. a bundle of all property rights' whereas in common law gradual ownership of property is admissible.[573] It stems from this that in common law countries like the UK or the US, gradual ownership could reflect gradual control currently mandated by the GDPR. Unfortunately, 'we lack a word for describing control over things without legal or beneficial ownership of them - a word that signifies that the thing described is both not common and not owned'.[574] Gradual property rights would essentially give individuals control over personal data and most shortcomings of this approach, 'are likely to mirror the shortcomings of a data protection regime which places individual control at its core'.[575] Even though most EU Member States form part of the civil law system (in which property equals full ownership), defining personal data in terms of gradual ownership could be imposed in those countries as well through, for example, regulations adopted by EU institutions. What are the arguments in favour and against viewing personal data as property? How does the situation of vulnerable individuals influence this debate? What impact would defining personal data as property have on people's perception of personal data? Responding to these questions is essential in the context of PIMS systems the objective of which is to render practically effective the control over personal data by the data subject. As a consequence, the limits to data control and the concept of ownership should first be theoretically explored before delving into the question of how vulnerable people's data should be managed by PIMS architectures.

4.3.I.B Proponents of Data Ownership

Some have argued that 'property talk would give privacy rhetoric added support' in the specific circumstances currently predominating in countries like the United States, that is circumstances, in which (unlike in the EU and in the UK) the overall approval for a minimum protection attributed to personal data does not really exist.[576] As a result, the proponents of

[573] Václav Janeček, 'Ownership of Personal Data in the Internet of Things' (2018) 34(5) Computer Law & Security Review 1039.

[574] Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (n 274).

[575] Lynskey 237 (n 571).

[576] Lawrence Lessig, 'Privacy as Property' (2002) 69(1) Social Research: An International Quarterly of Social Sciences 247.

property rights in the US argue that this approach moves the lack of control over data processing performed by private companies to one where those who desire to process someone's data need to pay for the latter. However, this reasoning is not convincing in the EU where a thorough data protection regime has been adopted a few decades ago.[577] Currently, it might also be seen as less convincing in the US where certain States like California recently adopted more privacy friendly legislation (California Privacy Rights Act).

An argument that can be made in favour of viewing personal data as fully owned property rights is that they would give individuals more control over their data.[578] If personal data was treated as fully owned property, it would become alienable and give individuals the possibility to exchange it for a certain benefit and, therefore, in theory exercise more control over the latter. Companies might be more willing to pay for this data as they would know that they can acquire it without the possibility for data subjects to modify their decision or exercise certain rights such as the right of access. Whether this amount of control is desirable will be discussed in the next section. However, it seems that giving data subjects 'more control' in this context would also actually equate in practice to more easily losing all control over their data.

Advocates of the property rights approach sometimes underline that by giving data subjects the possibility to allocate a different worth to their personal data depending on the situation, the property rights approach would lead to an economically efficient and appropriate assignment of value to personal data as property. If a company assigns higher worth to personal data than data subjects, the latter will sell their data. If it's the opposite, data subjects would not allow their data to be processed.[579] This would lead to a regime of optimal allocation of personal data as a resource.

Finally, some researchers consider that the divisible nature of property would allow data subjects to benefit from the choice as to how they use their personal data. In fact, it is possible to assert that data subjects possess 'personal rights' over their personal data (the immaterial value of data attributed automatically to the individual) and 'rights of use' (related to how individuals protect their data's economic worth), thereby differentiating between moral and

[577] Lynskey (n 571).
[578] Ibid.
[579] Nadezhda Purtova, *Property Rights in Personal Data: A European Perspective* (Kluwer Law International 2011).

economic rights concerning personal data (similarly to intellectual property rights related to creative works).[580] This divisibility would permit individuals to benefit from the economic value of their personal data (right of use) and, at the same time, enable them to object to the processing of their data when the latter is detrimental to their personality rights. However, this would mean that neither the right of use is fully alienable, nor the personal right fully divisible and would more or less equate to what the GDPR offers at the moment, that is giving data subjects the right to benefit from the economic value of their data without sacrificing, for example, their right of access or to rectify their data. The main difference would lie in that personal data would be considered as property. Is this desirable?

4.3.I.C Arguments in Favour of the Fundamental Rights Approach

Before presenting this PhD's arguments against treating personal data as property, it should be noted that while the EU data protection regime gives data subjects rights to, for example, revoke their consent or to rectify their data, it is still a permissive regime in the sense that it does not discourage or prohibit trade in personal data. This trade is just more limited than in a property rights regime permitting full ownership and no limitations to what one can do with their data. However, what about common law countries such as the UK or Ireland, which allow gradual property rights? In this sense, a gradual property rights regime could seem similar to what the GDPR control regime proposes. Why does this thesis argue in favour of never considering personal data as property regardless of whether this would entail full or gradual ownership?

Firstly, it is not self-evident why a liberalised market (implicitly supported by the property rights approach) would result in the optimal allocation of scarce resources in the context of personal data being them. Whether such a purely economic and market-oriented approach should be used for a fundamental right is objectionable. Allowing companies to acquire full ownership of their consumers' data could legitimise the most questionable personal data processing activities. As some have stated, 'market solutions based on a property rights model won't cure it; they'll only legitimize it'.[581] For example, if persons regarded as having waived all property rights in their information transferred to certain companies in return for special

[580] Samuelson Pamela, 'Privacy as Intellectual Property?' (2000) 52(5) Stanford Law Review 1125; Lynskey 236-237 (n 571).

[581] Jessica Litman, 'Information Privacy/Information Property' (2000) 52(5) Stanford Law Review 1283, 1301.

rewards should unexpectedly become vulnerable due to an illness, which they would not like to disclose, they may not possess any practical way to regain their secrecy.

While the GDPR does emphasise the importance of control, the current provisions seem to prohibit data subjects from waiving their rights granted by the EU data protection framework when signing data processing agreements. Individuals may not be deprived of their data but they can control it to a certain extent and, for example, license its use to a third party. As an example, a person could consent to data processing but it is improbable that a court would consider legal, the terms of an agreement preventing this person from exercising their right to rectify or access personal data (subject to specific exceptions such as in the case of public figures when information about them is considered newsworthy).[582] Personal data cannot be such an exception. This would go against the directly applicable GDPR, a regulation with provisions leaving little room for interpretative legislative manoeuvre. The GDPR strives to ensure that consumers' personal data is safe while giving them more control over their data at the same time. Data subjects can take various decisions in relation to how their data is processed and, in principle, they always have the ability to change them. Property viewed as full ownership of personal data would imply the possibility of selling this data to third parties and losing all control over it, which is not allowed by the GDPR and, according to this PhD, is not desirable in general. This would also probably go against the still largely unexplored fairness principle. If, for the latter, maintaining a balance between the rights and powers of companies and individuals is essential, then vulnerable consumers must always be able to exercise their GDPR rights. This is subject (as previously argued in this chapter) to other considerations such as the prevailing importance of vulnerable people's data confidentiality over other rights they may have. However, it should not be subject to a company's decision to acquire a person's data. Moreover, and even when disregarding GDPR's clear stance on the necessity to take special care of vulnerable people's personal data, it seems intuitively right not to allow full ownership of personal data, especially when vulnerable individuals' needs are taken into consideration. Consumers can be easily manipulated into making harmful choices if data protection provisions are not complied with. They are often not aware of the intricacies of data processing.[583] Vulnerable individuals should not be put in a situation (even voluntarily) where

[582] Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, [2015] (ECLI:EU:C:2014:317).

[583] Corien Prins, 'Property and Privacy : European Perspectives and the Commodification of our Identity' in Lucie Guibault and Bernt P. Hugenholtz (eds), *The Future of the Public Domain, Identifying the Commons in Information Law* (Kluwer Law International 2006) 252.

they must decide whether they should give away their data in exchange of a service or reward. They cannot be expected to understand all of the consequences that would be associated with such a decision.

The President of the CJEU has asserted that the 'the concept of the essence of a fundamental right - set out in Article 52(1) of the Charter of Fundamental Rights of the European Union (the "Charter") - operates as a constant reminder that our core values as Europeans are absolute', including data protection.[584] The *Schrems* judgments confirmed this by underlining that when a measure introduces a limitation on the exercise of a fundamental right that is so great and far-reaching that it denies the existence of this right in practice, that measure contradicts the Charter's provisions.[585] There is no necessity to conduct a balancing exercise of the different interests involved. A measure that calls into question the essence of a fundamental right is automatically disproportionate.[586] The seminal 2015 *Schrems* case is the first one in all of CJEU's jurisprudence where the court holds that a Union measure (the Commission's Safe Harbor adequacy decision) breaches the essence of a fundamental right.[587] This shows how important it is for the highest EU Court to prevent any attempt at separating the fundamental data protection right from its essence. For this concept to operate in a constitutionally meaningful manner, courts and other actors should apply the 'respect-for-the-essence test' before conducting any proportionality assessment test.[588] If personal data should not be thought of as a 'thing' owned by individuals, how should it be conceptualised? What does fundamental right mean in the context of personal data?

According to Cohen, philosophers and legal scholars have tried for decades to find a convincing definition of privacy in different terms, 'as a locus of personal or dignitary interests'.[589] This language may seem blurred and unclear to some, and it may be difficult to set the boundaries of our dignity. However, the property rights approach, which favours 'boundedness, even at the risk of oversimplification' should not be applied concerning personal data.[590] The privacy as dignity approach may seem fuzzy but, according to this thesis, it is unquestionable that data is indeed linked to human dignity and to the essence of one's self.

[584] Lenaerts (n 570).
[585] *Schrems (n 558)*.
[586] Lenaerts (n 570).
[587] *Schrems (n 558)*.
[588] Lenaerts (n 570).
[589] Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' 1380 (n 274).
[590] Ibid.

Oversimplification of the concept of personal data and what it means for individuals could be dangerous. Personal data concerns intimate aspects of our lives and its protection is necessary for our psychic well-being, development and social relationships.[591] Some have argued that 'the concept of (commercial) property may not be vested in privacy because privacy is attached to individuals by virtue of their personhood, and, as such, this right cannot be waived or transferred to others (either for commercial or for other reasons)'.[592] Cohen considers that waiving privacy can negatively affect the development of selfhood.[593] As a consequence, it should not be viewed as a commodity that can always be traded for other goods. Just as we cannot sell our blood or DNA, we should not be able to completely let go of our personal data and, therefore, have full ownership in a property rights sense of the latter. Our data is part of who we are as human beings. Allowing individuals to irreversibly separate themselves from their personal data and losing all control over it would, according to this thesis, violate the respect-for-the-essence of a fundamental right test. This point of view is confirmed by current provisions and the inalienability of human rights in EU law to which there are exceptions in only limited circumstances.[594]

The inalienability of fundamental rights is based on the concept of human dignity. For some, this means that dignity is used as constraint rather than empowerment, as it limits what individuals can do with their data.[595] However, when one takes into account the situation of vulnerable individuals such constraint can equal empowerment. By prohibiting individuals from fully alienating their personal data, the GDPR also better protects vulnerable people who may not be conscious of the risks involved and empowers them by letting them keep the ability to exercise their data protection rights and protecting their data against malicious actors. Data will never be a 'normal' product. Most people can understand the consequences of selling a car but it would be difficult for any person to fully grasp and predict the consequences of irreversibly letting go of one's personal data.

[591] Jerry Kang and Benedikt Buchner, 'Privacy in Atlantis' (2004) 18(1) Harvard Journal of Law & Technology 229, 234.

[592] Prins 234 (n 583).

[593] Cohen, *Configuring the Networked Self* (n 460)*;* Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' 1895 (n 460).

[594] Prins (n 583); Lynskey 241 (n 571).

[595] Lynskey 242 (n 571).

Another conceptual obstacle to defining personal data as property is that personal data is non-rivalrous.[596] The same personal data may concern several data subjects and, according to some, it is always to some degree created by more than one person.[597] For example, a picture can contain personal data of a multitude of people. This creates issues related to property rights' assignment. Of course, this is a problem that also exists in the framework of GDPR's control regime, the latter allowing extensive control of personal data by individuals. However, not to the same extent that property rights might do. Giving individuals full ownership of a picture containing personal data related to several persons would allow selling such a picture, and could create much more pronounced issues if consent of the other data owners has not been obtained. Moreover, this would mean full ownership does not really exist as other people in the picture should fully own the data as well but would not be able to protest if it is sold.

The way in which people conceptualise and debate personal data is important as well. If society frames the question of personal data as property rights instead of a data protection or privacy problem, this could lead individuals to consider their data more 'like their car than their soul'.[598] If a property rights regime was to make data protection rights of data subjects more effective, there could be a conflict between those who idealistically argue against this approach and those who pragmatically consider the most effective solution. However, as this thesis has discussed above, the property rights approach has various flaws and is not a convincingly more effective solution from a conceptual perspective. For this reason, the argument in favour of framing data as a fundamental right instead of a property right in public discourse can only reinforce the conclusions of this section.

As it has been mentioned before, the objective of PIMS is to give data subjects control over their personal data and enable them to exercise their GDPR rights more easily. In this section, this thesis has argued that personal data should not be viewed as property, especially when vulnerable people's needs are taken into consideration. In the next one, it will discuss to what extent vulnerable data subjects should have control over their personal data and to what extent this control should be limited. How can PIMS support vulnerable persons and their legal

[596] Mireille Hildebrandt, 'Balance or Trade-off? Online Security Technologies and Fundamental Rights' (2013) 26(4) Philosophy & Technology 357, 367.

[597] Ferretti 848 (n 138).

[598] Kang and Buchner 260 (n 591); Lynskey 238 (n 571).

guardians in the management of their data gathered by smart devices and how can they help companies with GDPR compliance?

4.3.II Managing Vulnerable People's Data Collected by Smart Devices

Vulnerable people need to be supported in data management processes (4.3.II.A). To what extent should they be able to process other people's data gathered by smart products and present on their PIMS (4.3.II.B)? This section also discusses legal guardians' and parents' role in managing vulnerable individuals' data in the context of PIMS and smart homes (4.3.II.C). It analyses the question of data monetisation by vulnerable people and by their legal guardians (4.3.II.D). Finally, the topic of how the legitimate interests legal basis could be used by companies instead of consent within the PIMS ecosystem is evaluated (4.3.II.E).

4.3.II.A Supporting Vulnerable Individuals in Securely Controlling their Own Data

If giving control to the user is in conformity with the spirit of the GDPR, this thesis has previously shown that it is not necessarily always the right choice. Guaranteeing the security of children's and vulnerable adults' data with special measures is also what the regulation strives to achieve. First, the confidentiality and integrity of their data should be ensured. As it has been argued in the doctrinal study, this is a prerequisite for lawful data processing. Assuming that vulnerable people's data is indeed well secured, what kind of decisions should they be allowed to take in relation to their data when managing smart devices? How do PIMS operate in this context?

The majority of people using products such as IoT devices are not opting out as companies process their personal data. They are 'exposing the intimate minutiae of their lives on sites like Facebook and Twitter', as well as through smart devices.[599] However, this rise in sharing data is not the consequence of people's choices but also, in part, a consequence of the fact that many smart products are designed in a way that promotes data sharing and limits understanding of the risks involved. This issue is made even more acute because of the many children, teenagers and vulnerable adults whose capacity to make informed choices may be lower than that of other citizens. One of the main objectives of PIMS is to allow the user to take more meaningful

[599] Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' 1895 (n 120).

decisions concerning the dissemination of their personal data.[600] PIMS are making it possible for consumers to determine which personal computations they will give permission for and which collective computations they will agree to participate in. However, to what extent this is appropriate in the context of vulnerable individuals?

In corporate environments, data management decisions would be administered by central authorities with the help of IT experts who determine suitable roles, define access control policies, and ensure security and auditing measures are in place to prevent any potential issues.[601] In the PIMS smart home context, it is exactly the reverse. The responsibility of taking appropriate decisions and their enforcement is handed to users of smart devices. This leads to risks for vulnerable people. Some authors argue that 'we should be cautious of a potential boomerang effect of user empowerment' when giving individuals more liberty without providing the right environment to exercise control over their data.[602] Certain access control models are not well suited for a vulnerable and untrained audience having to administer a very dynamic group of interactions with a multitude of third parties and different users.[603] They require consumers to manually choose all of the basic sharing rules and make them manage cryptographic protection. As a result, some argue that people could be overwhelmed and decide to rely on centralised service providers for the management of their data.[604] This would go against the very essence of PIMS the objective of which is to empower and give back control to the user as well as prevent third parties from gaining access to a person's digital record.

A solution would be for PIMS settings to minimise data sharing by default without requiring the individual to take any important decisions at the initial stage of using a product or service. Any non-essential data processing decision should require an opt-in and active engagement of the user. All optional data processing should be turned off by default, taking into consideration the intrinsic weaknesses of vulnerable people and, at the same time, giving them control over their data if they wish to change those settings. The necessity to change them would inherently

[600] Anciaux and others (n 493).
[601] Ibid.
[602] Ibid.
[603] Barbara Carminati, Elena Ferrari and Andrea Perego, 'Rule-Based Access Control for Social Networks' in Springer LNCS (ed), *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops* (Springer Berlin Heidelberg 2006) <https://dx.doi.org/10.1007/11915072_80>.
[604] Paul Tran-Van, Nicolas Anciaux and Philippe Pucheral, 'SWYSWYK: A Privacy-by-Design Paradigm for Personal Information Management Systems' (International Conference on Information Systems Development(ISD), Cyprus, September 2017).

result in more informed choices. Moreover, one of the current problems related to the development and deployment of billions of smart products is compliance and enforcement of the GDPR. There are thousands of IoT companies producing smart devices without meeting data protection requirements. If a vulnerable person's smart home products were integrated into a PIMS in which data processing is turned off by default, this would automatically increase companies' GDPR compliance and help in protecting vulnerable people's data.

In Chapter 2, this thesis has underlined the fact that many smart devices do not communicate their privacy policies and users' data protection choices in a transparent way. For example, many IoT products do not have any user interface and do not provide their users with an easy option to learn about or modify their privacy settings.[605] By managing all of their data on a single device (the PIMS), vulnerable people would not need to worry about choosing settings on all of their devices separately and they could benefit from a much more usable interface, with dashboards which visualise datasets to vulnerable users in a more comprehensible manner.[606] PIMS have been also suggested as a potential solution to support the data subject in dealing with granular consent. The fact that it is only one device would surely make the settings more familiar and easier to change over time, instead of the current device interface heterogeneity that characterises the smart home environment.

4.3.II.B Protecting Vulnerable Subjects from Mishandling Other People's Data by Mistake

Issues regarding data control do not only concern the PIMS owner's personal data but also personal data of other people stored within the system. Art. 82(2) GDPR states that 'Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation'. According to Rec. 85 GDPR the damages can consist of a 'loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned'. Can a vulnerable person be liable for the damage caused by processing other people's personal data on its PIMS?

[605] Gruman (n 187).
[606] Urquhart, Sailaja and McAuley (n 568).

A PIMS can store personal data of various persons such as, for example, contact details of doctors gathered by a smart health product. In principle, PIMS should guarantee data's confidentiality on behalf of the vulnerable consumer. However, what if the vulnerable consumer accesses personal data of other individuals through the system and decides to send it to untrusted third parties. In this scenario, is the vulnerable person a data controller liable for the damage they have potentially caused?[607] Vulnerable individuals should not be in a position where they are faced with difficult choices regarding other people's personal data. For this reason, this PhD considers that PETs should block the possibility of undertaking certain actions with special category data. For example, vulnerable users should be capable of accessing the contact details of their doctors gathered by smart products and stored inside the PIMS but not be able to send this data to third parties. For some authors, such restrictions should be extended to all owners of PIMS and not only vulnerable individuals. They argue that consumers should not be given access to all of the PIMS content.[608] From the point of view of an organisation's interests, this would ensure better data protection compliance. Moreover, this would make the problem of differentiating between an ordinary citizen and a vulnerable person disappear. However, the question lies as to where exactly the line should be drawn between data that can be fully controlled and data for which certain actions should be prohibited. What kind of actions should individuals be able to undertake regarding other people's personal data stored on their PIMS? There is no easy answer to this question but designers and developers of the PIMS hardware and software should cooperate with lawyers to find the most GDPR compliant solutions. In general, this thesis considers that the answer should be the minimum amount of data possible without previously obtaining the consent of the data's true owner. In most cases, transferring other people's data should not be needed unless a person previously entered, for example, in a contractual agreement that requires such transfers in which case there will already be a lawful legal basis.

4.3.II.C Limiting Parents' and Legal Guardians' Data Management Powers

[607] Users of smart home devices may have lawful reasons to process others' personal data, including for a legitimate interest pursued by themselves, whether for a domestic purpose or not. For a discussion on how smart home-owners might be held responsible as a data controller without being covered by the household exemption provided by Art 2.2 (c) GDPR, see Chen and Urquhart, 'On the Principle of Accountability: Challenges for Smart Homes and Cybersecurity' (n 544).

[608] Anciaux and others (n 493).

Personal data is often related to several persons and not one individual. It cannot always be easily separated. Each data point does not always belong to one person. Data means relationships and can concern not only the 'me' or 'you' but also 'us' and, as a consequence, the consistency of the 'my data' model begins to fall apart.[609] As mentioned before in this chapter, data could be owned by a group of people (such as a family picture). In these circumstances, decisions as to who can be granted access to the data may be required to reflect the expectations and preferences of every member of the group. This is also the case in the context of vulnerable adults or children. In a smart home, personal data will reside with the persons from whom the data has originated but control could be temporarily entrusted to a different individual (such as a parent or legal guardian) to handle, for example, a vulnerable adult's health record gathered through a smart product.[610] As a consequence, vulnerable users of PIMS do not necessarily possess the privileges required to control their data stored inside the platform.[611] Parents might be in control when their child is underage, a legal guardian when adults are vulnerable or the system could be simply set up giving control to a specific person in the household. A PIMS can gather all of smart homes users' personal data and they need to be protected from each others' unintended (or intended) actions. If a person does not have the capacity to make informed data processing choices, when should a legal guardian be able to act on behalf of this person?

Some consider that parents are not best suited and should not be trusted to ensure their children's protection online, 'as many are unaware or unable to mediate their children's online activities'.[612] Parents do not always have the best answer and possess the digital literacy skills needed to effectively manage their children's data. One paper has shown that many adults consider that their children comprehend the online world better than them and are not always well suited to provide specific, freely given, informed and unambiguous consent, as they are often not accustomed to the services that the younger generation wishes to use, or do not have the required time nor patience to understand them and their associated privacy policies. This

[609] Andy Crabtree and Richard Mortier, 'Human Data Interaction: Historical Lessons from Social Studies and CSCW' (ECSCW 2015: Proceedings of the 14th European Conference on Computer Supported Cooperative Work, Oslo, 2015); Perera and others (n 498).
[610] Crabtree and Mortier (n 609).
[611] Anciaux and others (n 493).
[612] Sonia Livingstone and Leslie Haddon, 'EU Kids Online' (2009) <http://eprints.lse.ac.uk/24372/1/EU%20Kids%20Online%20final%20report%202009%28lsero%29.pdf> accessed 1 July 2022; Milkaite and Lievens, 'The Internet of Toys: Playing Games with Children's Data?' (n 440).

leads to the question of whether consent is really informed when provided by them.[613] The same issue can be raised concerning legal guardians taking care of vulnerable adults.

Independently of legal guardians' and parents' capacity to make informed choices, another issue are their good intentions. While most of them are likely to have the best interests of the vulnerable persons under their protection as the top priority, this will not necessarily be the case in every household. In June 2018, the New York Times published an article in which it warned against the increasing number of IoT products involved in domestic abuse cases.[614] The article brings attention to the imbalance of power created by IoT products within smart homes. The author mentions individuals calling hotlines worried about what is happening within their household. For example, a woman in distress informed the hotline that code numbers to enter her home change every day and she does not understand why. This is an example of a new form of domestic abuse through smart devices used to harass or monitor other smart home dwellers. IoT devices create the opportunity for bad actors to remotely control smart products to abuse their victims. This kind of power could also be used in relation to vulnerable people and their data. While domestic abuse may be a problem that is not easily solved by any kind of PET, some issues linked to the processing of vulnerable individuals' data for malicious purposes by other members of the household could be prevented and limited through the design of PIMS systems.

If legal guardians have access to all of the vulnerable person's personal data present on a PIMS, and if they can use smart devices to process even more data about them, they could potentially abuse this power. Access to vulnerable people's personal data should be more limited than the access a PIMS owner has to their own data. Unless this is required by law (for example, for health-related reasons) or unless they have given their informed consent (if this is possible depending on their condition), the legal guardian or parent should be prevented from processing vulnerable people's data. While this may not solve the issue of harming victims by using smart devices in abusive ways (such as the above-mentioned example of changing the door lock everyday), it could at least protect vulnerable individuals against excessive collection and processing of their data without their approval. For example, if people's voices are collected

[613] Simone van der Hof, 'I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2016) 34(2) Wisconsin International Law Journal 409.

[614] Nellie Bowles, 'Thermostats, Locks and Lights: Digital Tools of Domestic Abuse' (*The New York Times*, 2018) <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html> accessed 1 July 2022.

by a smart home assistant and this data is present on the PIMS, the PIMS owner should be able to manage recordings based on his own voice and not the other household members' voices unless they consent to it. Recordings where several persons speak would therefore require the consent of all of those persons. Access to them should be prevented by default. One question that arises is how the PIMS would know how many persons live within a smart home? How would it know to whom a particular piece of data belongs? How would the device be informed as to who has consented to data processing? These are open questions that new technological developments need to find a response to.

Similar issues also appear in the context of data monetisation, an important topic in the context of PIMS as the latter need new business models for their widespread adoption to materialise.

4.3.II.D Monetising Vulnerable Users' Data

Current business models of monetizing people's data are mainly based on centralised cloud architectures. The approach of monetizing data through cloud models is reflected in smart homes, 'with personal data collected by IoT devices typically being distributed to the cloud for processing and analytics'.[615] However, some researchers have recently noted that new payment mechanisms are appearing in relation to data and privacy-related purchases, and this in context of edge computing architectural models.[616] Indeed, 'making personal data available for access and trade is expected to become a part of the data driven digital economy'.[617] New manners of exchanging data generated at the edge of the network for new services should emerge and it is expected that entities that gather this data will pay the services at the edge from which it has originated.[618] PIMS need to create value for all stakeholders in order to be successful. Trading data will be important for the survival of PIMS as it could enable their more widespread adoption. How should this value creation work in the context of vulnerable persons using smart devices?

[615] Urquhart, Crabtree and Lodge (n 468).

[616] Wired, 'Decentralised AI has the Potential to Upend the Online Economy' (2021) <https://www.wired.co.uk/article/decentralised-artificial-intelligence> accessed 1 July 2022.

[617] Perera and others (n 498).

[618] Wired, 'Decentralised AI has the Potential to Upend the Online Economy' (n 616).

The sensing as a service model envisages the development of a data marketplace for people who want to allow access to their personal data for a reward and for those interested in receiving this data (data consumers).[619] Metadata about vulnerable individuals' personal data stored on the PIMS could be made available and commercialised in the market place after obtaining their approval. Alternatively, and similarly to the current mobile app market, data consumers could announce offers and data enrolment opportunities themselves, and data owners could subscribe for their data to be processed for a set amount of time. For example, let's imagine data collected from a person's thermostat or smart fridge is transferred to their PIMS. From a sensing as a service perspective, this person could be prepared to give access to their data to a third party in exchange for a reward. This reward could be money, discounts, loyalty cards or any other gift of value to the data owner. This could be done by either announcing on a marketplace their willingness to rent their data or by responding to a data consumer offer already present on this marketplace. Apart from possible rewards for data subjects, these kinds of economic exchanges will be important to attract companies to PIMS and to show them that they will also increase their revenue when using this kind of architectural model.

While temporarily allowing a third party to process data in exchange for rewards is arguably an acceptable practice under the GDPR provisions on data portability (Article 20), this should be done with caution as trading special category data could expose individuals' intimate details of their personal everyday life to unknown entities.[620] For example, if their smart health devices transfer data to third parties and those third parties do not have effective data protection mechanisms in place or sell this data to insurance companies (to establish consumer profiles), this could potentially negatively affect vulnerable persons. Both 'ordinary' data and metadata can contain a lot of information about a person and their habits. If a certain PIMS allows data monetisation, it should also contain mechanisms preventing monetisation by untrustworthy external organisations. Companies that want to buy data could be required to undergo a quick security check before they are allowed to do so. Edge architectures may have the best intentions of giving users more control but this should not be done at the expense of their safety and security.

[619] Perera and others (n 498).

[620] Urquhart, Sailaja and McAuley (n 568).

In any case, this thesis considers that legal guardians and parents should not be allowed to monetise data of the vulnerable people under their protection. PIMS should find a way to prevent them from doing so. The power they have to manage vulnerable individuals' data should not be used for their own benefit and at the expense of those they are supposed to protect. As it has been mentioned above, parents, for example, often do not understand the intricacies of personal data processing and, even if they have good intentions, they might not be able to comprehend the consequences of selling their children's data to third parties. For this reason, monetising a vulnerable person's data should only be allowed, according to this PhD, when vulnerable persons are capable of providing informed consent themselves.

4.3.II.E Data Control and the Legitimate Interests Legal Basis

How should PIMS respond when organisations process children's and vulnerable adults' personal information using the legitimate interests legal basis? How to make sure that vulnerable individuals do not unknowingly lose control over their data when this legal ground is used? Other legal bases discussed in this thesis (in particular, performance of a contract and consent) might also be used but the limits they pose to companies' data processing activities are clearer than in the case of legitimate interests. Some authors worry that legitimate interests could mean 'that just about anything goes' in terms of justifying and finding a legal ground to process people's personal data.[621] Instead, they underline the importance of the fairness principle (Art. 5 GDPR), which requires organisations to be transparent and, as a result, seem to argue in favour of consent as being a more transparent process. Moreover, researchers bring attention to the fact that in PIMS architectures other grounds than consent are less considered.[622] Indeed, installing apps for data processing and deciding on preferences in terms of data usage and policies to allow such processing, signifies that consumers need to actively participate – that is take deliberative actions – for the processing to actually happen. The technical design of PIMS platforms, 'which require active user action for processing to occur, seems to be oriented towards supporting consent and contract-based processing'.[623] What does not seem considered in PIMS architectures are the bases that do not rely on specific data subject's agreement. The legitimate interests legal basis does not necessitate the consumer's agreement for data processing to occur.

[621] Crabtree and others 41 (n 165).
[622] Janssen and others (n 471).
[623] Ibid.

The lack of transparency and power imbalance related to legitimate interests and the fact that PIMS have not considered how to deal with this legal basis are valid concerns. The former has been discussed in the doctrinal chapter while the latter is an important topic in the context of PIMS architectures. Big companies such as Google produce many smart products and use legitimate interests to process data more and more often.[624] There is an inherent imbalance of power between a vulnerable consumer and a data controller, but this legal basis will continue to be widely used. In principle, there is no reason why adopting legitimate interests would result in a less transparent process than consent. Indeed, transparency is a horizontal requirement that should also apply to this legal ground. Companies are required to balance their rights against data subjects' data protection rights and to take into consideration vulnerable people's needs. However, this is often not done correctly in practice. PIMS need to have an adequate response.

The current technical design of PIMS platforms assumes that data processing will take place if the user explicitly allows this to happen (for example, by setting preferences, installing an application etc.). As a consequence, it is not certain how PIMS workings can be reconciled with the lawful data processing grounds which do not necessitate user involvement. Some underline that 'this is an area that has received little consideration, and one requiring further attention'.[625] Technical mechanisms currently offered by PIMS platforms could possibly be developed to assist other kinds of legal bases and ensure their lawful and effective adoption.[626] For example, transparent information about a controller's legitimate interests as a processing ground could be provided to consumers through comparable means used to present other information to them, such as clear online notices or installation processes.[627] When an organisation decides to process personal data based on legitimate interests, PIMS could promote the use of transparent communication mechanisms, which would hopefully create more awareness about the data processing activities that take place.

In Chapter 2, this thesis has underlined that organisations need to take 'extra care' to protect children's (and vulnerable adults') rights and freedoms from data processing risks and effects

[624] Ferretti (n 138).
[625] Janssen and others (n 471).
[626] Ibid.
[627] Ibid.

if they wish to use the legitimate interests legal ground to process their personal data.[628] It has also expressed concern as to whether organisations will in practice perform effective balancing exercises if they do not fear enforcement action. Legitimate interests can be an appropriate legal ground when an organisation decides to process personal data in ways that the data subject would reasonably expect and that have only minimal influence on privacy, or when there is a convincing explanation for the processing.[629] Because effective enforcement is difficult, PIMS could potentially help in greater GDPR compliance in this context. This topic should at least be researched in more depth by computer scientists in collaboration with lawyers to evaluate whether the current situation of ineffective balancing exercises often performed by organisations could be partially resolved by using PETs. For example, if certain smart toys were to process children's data and establish profiles of children based on a company's legitimate interests, PIMS could automatically notice such activity and stop it as profiling of children is in general prohibited. Flagrant violations of the GDPR through illegal data processing of vulnerable individuals' data based on legitimate interests could possibly be stopped by PIMS if technological developments allow the identification of such violations. The benefit of PIMS is that all of the smart home is supposed to be connected to it and, therefore, the protection would be extended to all devices.

Moreover, consumers' data protection preferences might not reflect the controller's legitimate interests. There could be a mismatch between the former and the latter.[630] Consumers might not want their data to be processed based on controllers' legitimate interests. Some consider that how this can be resolved in a PIMS context, considering the nature of PIMS architectures, needs more research and analysis.[631] Maybe PIMS could automatically prevent the processing from taking place if they notice unusual data processing requests based on the user's privacy preferences (thereby also facilitating the exercise of the right to object, Art. 21 GDPR). As a result, they would contact the data subject who would then need to explicitly agree for the processing to continue or object to the data processing. Consent mechanisms could be repurposed and adapted to such situations where processing based on legitimate interests does not reflect data subjects' choices. The balancing exercise should be stricter when vulnerable

[628] Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (n 26); Information Commissioner's Office, 'Legitimate Interests' (n 141).
[629] Ibid.
[630] Ferretti (n 138).
[631] Janssen and others (n 471).

people use smart products, which is another argument for making sure that the interests of the company reflect the interests of vulnerable consumers.

Section 4.4 Chapter's Summary and Conclusion

Technologies have an undeniable impact on how people behave in the online world and, as a consequence, on what they can and cannot do with their data. A set of technical approaches have emerged under the name of privacy enhancing technologies to promote safer and more effective processing of personal data. PIMS are one type of such technologies, with the particularity that they strive to offer a full solution to GDPR compliance requirements. This thesis has focussed on edge computing PIMS. While relying on the cloud was historically justifiable, current technological developments permit edge computing systems to offer the same benefits as cloud-based systems. Both architectures can offer efficient computing utility or storage, virtualisation and access to services through networking, while edge computing has the added security benefit of processing data locally. There is a certain momentum that needs to be recognised in favour of decentralised data processing. The European Commission has mentioned this type of processing as a potential opportunity to improve data control and management. The issue with edge systems is their current lack of widespread adoption. There must be incentives - such as governments leading through example by adopting those systems within their structures or new ways of monetising data gathered at the edge – that will convince organisations to use and implement edge computing PIMS.

In terms of data protection by design, current privacy enhancing technologies seem to focus on privacy-as-confidentiality as opposed to privacy-as-control. Some authors have criticised this approach as it impedes data subjects' capacity to exercise their rights and to manage data risks themselves. If a company does limit the possibility to exercise certain data protection rights, it should certainly justify this, for example, through DPIAs. However, this PhD considers that if an organisation is transparent about its privacy by design measures and their implications, and if a compromise needs to be made, prioritising privacy-as-confidentiality could be the right solution in the context of vulnerable individuals using smart products. The confidentiality of their personal information will be probably more important than the exercise of certain GDPR rights (such as the right of access). A solution to this inherent tension between privacy-as-confidentiality and privacy-as-control could be edge computing PIMS as they can offer both enhanced confidentiality and increased data control. From a security perspective, processing data locally signifies that raw data is stored at the network's edge, which prevents the risks intrinsic to cloud data computations. Only data necessary to respond to particular queries is sent to third parties. Moreover, in the case of edge architectures, functioning does not rely on uninterrupted connectivity, which increases a smart home's resilience and the protection of vulnerable citizens. In addition, edge computing PIMS detect unusual activities and data processing based on unusual data requests will not take place unless user's consent is obtained. The fact that data is processed at the edge also facilitates compliance with the data minimisation principle. When obtaining information on users' age or identity (for example, to establish whether a particular person is a legal guardian), the problem of potential excessive data collection by data controllers would disappear as PIMS would transmit only the required information (confirmed age or identity) to the relevant third party.

Apart from the confidentiality improvement, edge computing PIMS also strive to increase data subjects' control over their data. But what does control signify? This thesis argues in favour of considering data as an inalienable right instead of a fully or gradually owned property right, and this for several reasons. Among others, allowing organisations to acquire full ownership of people's data would legitimise the most questionable data processing practices as vulnerable consumers could be easily manipulated into making harmful and irreversible decisions. Moreover, this thesis considers that personal data is linked to our dignity, self-hood and essence of who we are as human beings. As a consequence, it should not be viewed as a commodity and people should not be able to sell it the same way as they are able to sell their cars or other tangible goods. Dignity in this context should not be perceived as a constraint but rather as empowerment. By preventing vulnerable individuals from fully separating themselves from personal data, this conceptual stance also protects them from giving up their rights and losing the ability to exercise control over their data. The way in which people debate personal data is essential as well and framing the latter as a property rights issue instead of a fundamental rights problem could lead society to reduce data to a commodity or common good, which, according to this thesis, should be avoided.

PIMS can empower users while switching off all unnecessary data sharing settings by default. The fact that such systems enable the management of various smart devices at the same time through a single transparent interface could facilitate vulnerable people's or legal guardians' potential decisions to opt-in to data processing. PIMS can store personal data of several persons. For this reason, this thesis argues in favour of restricting what a vulnerable person can do with other people's data stored within a PIMS to the minimum legally required (for example, accessing contact details of a doctor), unless consent has been previously obtained. Similarly, parents' and legal guardians' data management powers should also be limited through the PIMS design. Some argue that parents are not the best suited and should not be entrusted to ensure their children's data protection online. Moreover, legal guardians could misuse data of the persons they are supposed to protect. For this reason, reducing their data management powers seems like the more responsible approach. This raises the technical issue of how PIMS systems will know, which data can be accessed and processed by a legal guardian. Finally, while PIMS should offer possibilities of data monetisation to promote their widespread adoption, legal guardians should not be allowed to monetise data of vulnerable people as even if they have good intentions, they might not be able to predict the negative consequences that such monetisation could cause. Only if a vulnerable individual is capable of providing consent, their data monetisation should be allowed through PIMS systems.

It is worth mentioning that PIMS architectures and the literature related to those systems have mainly explored the consent legal basis while other legal grounds for processing have not been evaluated. This is especially relevant in the context of legitimate interests as the latter allows data processing without informing data subjects as long as a balancing exercise of data controllers' interests against those of vulnerable people has been done appropriately. However, as this thesis has discussed, there is a real risk that data controllers will ignore the stricter requirements of effective balancing exercises when vulnerable people's data is processed. PIMS could potentially help in this situation. For example, they could automatically stop flagrantly illegal data processing activities based on the legitimate interests legal basis (such as profiling children through IoT devices) or, when there is an obvious mismatch between a data subject's usual privacy preferences stored within the PIMS and the controllers' legitimate interests, ask for the user's consent before data processing is allowed.

In general, this thesis considers that there is a true opportunity with edge computing PIMS to reconcile privacy-as-confidentiality and privacy-as-control within a system that allows both to co-exist in a more harmonious manner. The increased data security, data minimisation and DPbDD that processing data at the edge enables can greatly support companies in meeting their

GDPR obligations. A widespread adoption of PIMS could facilitate GDPR compliance and increase the protection of vulnerable people's data and rights.

Chapter 5: PhD Conclusion

The conclusion will begin by summarising this PhD's main contributions before discussing its limitations and the associated need for further research.

Key Findings and Contributions

This thesis asked the question of how GDPR compliance works in theory and in practice when organisations develop and deploy smart devices used (or that could be used) by vulnerable people. This research question has been answered from three main perspectives: legal doctrinal, practical empirical and technological (grounded in normative debates).

In the doctrinal study, this thesis has reflected on the relevant legal grounds and their conditions when children or vulnerable people use smart products. Subsequently, other relevant GDPR principles have been critically analysed with the objective of comprehending how they should be complied with in this context. To better safeguard children's and vulnerable adults' fundamental freedoms and rights as well as support data controllers' compliance, this PhD argues in favour of preventing data protection problems by concentrating organisations' attention on the principles of data minimisation, security, data protection by design and by default (DPbDD) and on data protection impact assessments (DPIAs). When a data controller collects vulnerable people's data, this is exactly where issues might arise. For example, in the context of consent, satisfying its requirements and adopting special measures to safeguard vulnerable persons' personal data necessitates substantial effort and the more data is collected, the more problems can appear (in terms of organisations' GDPR obligations and for data subjects in relation to their rights). All security measures can be eventually overcome and risks of data breaches will never completely disappear. Of course, the appropriate implementation of a relevant legal ground remains essential when there is no other choice than to process personal data (such as when the health or well-being of consumers is at stake) or when data subjects have explicitly asked for their data to be processed. Controllers must ensure that they comply with all GDPR requirements before processing starts and that vulnerable data subjects can make truly informed choices. The decision regarding the appropriateness of a legal basis should be taken on a case-by-case basis. Regardless of the nature of the implemented legal ground, the data controller needs to adopt special data protection measures concerning vulnerable people and protect their fundamental rights and freedoms. This PhD argues that such measures should be adopted by default in every smart device. Any IoT product could be used by vulnerable persons and anyone could develop or intensify their vulnerability layers over time. Moreover, all citizens would benefit from those measures as they would enhance data protection and compliance in general. Apart from lawfulness, in the same GDPR provision, two other principles are discussed – transparency and fairness. They are overarching principles, essential to ensure an effective protection of vulnerable people's rights. There are various ways in which compliance with the transparency principle can be increased. In addition to communication mechanisms in relation to privacy policies, organisations could publish DPIAs showing that they have included vulnerable persons' considerations into them or, for example, adhere to codes of conduct such as ICO's Age Appropriate Design code and labelling schemes. In terms of the fairness principle, it is not yet well defined, which gives an opportunity to develop a definition encompassing data ethics initiatives as suggested by some scholars and the EDPS.

To verify how these topics have been considered by practising professionals, the study presented in Chapter 3 collected and analysed empirical evidence, which is currently lacking, from lawyers and technologists through semi-structured interviews. Their analysis confirmed and challenged findings of the doctrinal study, and inspired the theoretical and PETs-related debates in Chapter 4. The empirical chapter underlines the importance of promoting a vulnerability aware-approach (which would benefit all citizens and increase legal compliance) by defining unclear terms, educating and guiding organisations. Indeed, there is a need of a wider discussion to better define the notion of vulnerability (in particular, concerning vulnerable adults) and make it more tangible, to raise consumers' awareness about their rights (so that they can influence companies themselves), to develop sector specific guidance and support organisations in GDPR compliance, including through flexible (for example, by reducing fines if organisations self-declare violations) and adequate enforcement measures. Legal practical challenges were also evaluated in the empirical study. Legitimate interests and performance of a contract are preferred by companies because of the legal hurdles associated with consent. The extent to which the former will be beneficial for vulnerable people's rights and compliant with the GDPR will depend on the companies' willingness to perform in-depth balancing exercises (mainly due to insufficient enforcement measures). Transparency mechanisms should be adapted to various types of vulnerabilities by default, which is not always the case (for example, for visually impaired persons) and transparency requirements are still often ignored. The lack of a comprehensive definition of the fairness principle signifies that it is not applied in practice although it has the potential of being one of the most essential GDPR provisions, especially in the vulnerability context. Professionals expressed their wish for academics and courts to develop analytical frameworks in relation to fairness. Experts underscored the importance of some IoT devices for vulnerable persons' well-being (such as those monitoring whether an older adult had a fall or is in a health emergency) but also noticed the excessive data collection and the associated inferences made concerning consumers, the consequences of which could be exacerbated in the case of vulnerable people. Unfortunately, DPbDD obligations do not always seem well understood by some companies. The by default opt-in option frequently prevails over the legally required and desirable (especially for vulnerable individuals) opt-out by default measures. For experts, DPIAs should be more holistic exercises, which reflects this PhD's stance (developed in the doctrinal study) to use rights-based and values-oriented models that can be adapted to a particular data processing situation (for example, processing of children's data). Harmonisation in the field of standards and certifications is needed as well as their further development in the field of data protection and vulnerability. Such standards should not excessively impact smaller IoT companies, which could have difficulties in complying with their requirements in comparison to bigger organisations. Finally, interviewees also discussed technological issues and solutions linked to legal GDPR compliance. While security measures can never be perfect, they could have a dissuasive effect and most professionals agreed that confidentiality should be prioritised over control, not only because this diminishes their legal compliance hurdles but also because they consider this more important due to the situation of some vulnerable individuals living within smart homes. Accurate age and legal guardian identification (as also stated in Chapter 2) remains a crucial issue in the context of vulnerable persons and their data protection rights. One interviewee mentioned edge-computing computer vision systems as an example of a potential privacy-preserving solution for this conundrum as well as other problems discussed in the doctrinal and empirical studies. However, some professionals still think better smart device functionality can only be achieved with cloud systems, which remain widely adopted. Device interoperability is currently an issue but it is being worked on, in particular through a collaborative effort on the 'Matter' standard by the biggest IoT companies. This could push forward and change the smart home market landscape, both cloud and edge-based.

Finally, developing on the findings of the empirical study, the fourth chapter analysed the potential of edge-based solutions to improve GDPR compliance when vulnerable individuals use smart devices, those discussions being grounded in theoretical normative debates, which have problematised the implementation of technical solutions and opened up a space for a more nuanced discussion on some of the long-debated theories in the light of the particular challenges highlighted by edge solutions. Indeed, a set of technical approaches emerged under the name of privacy enhancing technologies to promote safer and more effective processing of personal data. Whether and how exactly these technologies can enhance privacy, however, depends on one's perception of what privacy means. In this regard, this thesis has looked at how two theoretical debates – 'confidentiality vs control' and 'property right vs inalienable right' – play out in the design of edge-based PIMS in practice when vulnerable people use smart products (PIMS, a particular kind of PET, have been analysed in-depth as they are data management systems providing both control and confidentiality, in line with GDPR's focus on control, as opposed to other PETs concentrating on the confidentiality aspect). While relying on the cloud was historically comprehensible, current technological developments allow edge computing models to provide similar benefits to cloud-based systems. A certain momentum in favour of the more privacy-preserving decentralised data processing has been developing over the last years. Using edge-based PIMS to process data offers new possibilities to better reconcile confidentiality and control as well as increase the security, data minimisation and DPbDD within smart homes. For example, in relation to the above-mentioned tension between the excessive data collection by IoT products and their usefulness for vulnerable individuals, edge systems can facilitate useful privacy-preserving data processing (such as, in the case of a bank's fraud detection app installed on a smart device, not revealing vulnerable users' exact location but only whether they are present where the suspicious activity is occurring). In the context of control, it is important to reflect on what this would mean in practice when PIMS are used by vulnerable individuals or their legal guardians. This thesis has critically analysed and proposed how to support vulnerable persons in securely controlling their own data (for example, by switching off all unnecessary data sharing settings by default), how to protect them from mishandling other people's data by mistake (by introducing certain restrictions on what can be done with other persons' data), and how (and why) parents' and legal guardians' data management powers should be limited as well (as they are not always the best suited or could misuse vulnerable people's data). If edge-based systems were to become widely adopted, it is important for their designers to take into consideration all GDPR provisions, including data processing based on other legal grounds than consent, which has been understudied in the literature so far. This requires an interdisciplinary approach and this thesis has proposed some solutions as to how PIMS mechanisms could promote compliance with the legitimate interests legal basis in order to enhance vulnerable people's data protection and reduce GDPR violations. Finally, the wider adoption of PIMS would also require new data monetisation mechanisms. However, this PhD considers that legal guardians should not be allowed to monetise data of vulnerable persons under their protection unless the latter are capable and willing to provide informed consent to such monetisation themselves.

Overall, this thesis contains a legal doctrinal chapter drawing attention to the need of thinking about vulnerability across all data protection principles and providing an in-depth analysis of GDPR compliance obligations in this regard, underscoring the importance of preventing issues through data minimisation, security, DPbDD and DPIAs; an empirical chapter, which verifies and challenges findings of the doctrinal study by interviewing lawyers and technologists working within the smart home field, giving a unique look into how professionals perceive and implement GDPR's provisions in the context of vulnerable people and the IoT; a chapter related to edge computing PETs (PIMS in particular), which offer enhanced data protection, data control and confidentiality to vulnerable consumers and legal guardians, and evaluating their potentiality and challenges in regard to GDPR compliance based on theoretically justified normative grounds. The interweaved nature of law and technology has been reaffirmed in this interdisciplinary study. Innovative technological solutions to legal problems are needed and many of the current legal issues are the result of companies' technological choices. In line with GDPR obligations, organisations developing smart devices must take vulnerable individuals into consideration within their processes and technological systems can support (or hinder) their efforts in this regard. This thesis is intended to serve as a basis for further discussions in this field and as a guide for both researchers and professionals interested in this topic.

Limitations and Further Research

In terms of this work's limitations, firstly, while in this thesis interviews were conducted with lawyers and technologists, it is a different matter what the expectations of vulnerable data subjects and their carers would be, what role their views should play in policymaking or to what extent data protection law should reflect their preferences when they do not necessarily fully understand the legal framework or the stakes involved. This PhD has focussed on the need to think about vulnerability across all data protection principles and on some technical solutions for which end users' input might have been difficult to obtain. However, while some issues may be too technical indeed, obtaining vulnerable data subjects' or their legal guardians' opinions on, for example, transparent communication measures or their involvement in DPIAs, could potentially improve certain aspects of GDPR compliance and their data protection. This study has not addressed these questions, which should be further investigated in future research and empirical studies.

Secondly, this thesis did not evaluate other kinds of laws and provisions, beyond the data protection law field of study. For example, the intersection between consumer law and data protection could be explored in the context of vulnerable individuals using smart products, and how their interaction would affect organisations' legal compliance obligations as well as consumers' rights. As some have argued, 'consumer law and data protection law can usefully complement each other' and further research in this area is required.[632] Intellectual property could come into play as well. Indeed, 'in an IoT world where personal data are appropriated by private companies by multiple means, including trade secrets, there is a palpable tension between data protection laws and trade secrecy'[633]. To what extent vulnerable people and their carers can rely on exceptions to trade secrecy to protect their data-related rights when they use new technologies such as smart devices? This is but one potentially relevant research question linked to intellectual property and this PhD's topic. Of course, there may be other fields of law, which should be delved into apart from consumer law and intellectual property (such as competition law) but the objective of this paragraph is simply to underline the need of future research in different legal areas.

Finally, the third limitation of this thesis is that it focussed on smart homes. The smart cities or smart hospitals settings are quite different and would require the consideration of other types of devices, policies, provisions and examples. As mentioned in the section on DPIAs, the prevailing values and rights of vulnerable data subjects will differ depending on where they use smart products. Equal treatment or civic engagement might be the most important values

[632] Frederik Zuiderveen Borgesius, Natali Helberger and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law' (2017) 54(5) Common Mkt Law Rev 1427.

[633] Guido Noto La Diega and Cristiana Sappa, 'The Internet of Things (IoT) at the Intersection of Data Protection and Trade Secrets. Non-Conventional Paths to Counter Data Sppropriation and Empower Consumers' (2020) 3 European Journal of Consumer Law 419, 457.

in a smart city while freedom of choice or the no-harm principle could prevail in a healthcare context. Exploring organisations' data protection-related obligations in public spaces or in medical environments would require a more detailed analysis of these particular settings. Considerations related to technological solutions, such as edge-based PIMS, would also need to be adapted to particular contexts. Some conclusions of this thesis may still apply but an in-depth evaluation of the specificities of these scenarios would be needed to implement the most effective solutions.

References

Brinkmann S and Kvale S, *Doing Interviews* (Flick U ed, 2 edn, SAGE 2018)

Cavoukian A, *Privacy by Design, Take the Challenge* (IPC Business Press 2009)

Cohen JE, *Configuring the Networked Self* (Yale University Press 2012)

Kosta E, *Consent in European Data Protection Law*, vol 3 (Brill/Martinus Nijhoff 2013)

Lessig L, *Code: Version 2.0* (Basic Books 30 December 2006)

—–, *Code and Other Laws of Cyberspace* (New York: Basic Books 1999)

Lynskey O, *The Foundations of EU Data Protection Law* (OUP 2015)

Mann T, *Australian Law Dictionary* (OUP Australia & New Zealand 7 January 2020)

Pasquale F, *The Black Box Society: the Secret Algorithms that Control Money and Information* (Harvard University Press 2016)

Purtova N, *Property Rights in Personal Data: A European Perspective* (Kluwer Law International 2011)

Schneier B, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World* (Norton 2018)

Von Grafenstein M, *The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation* (1 edn, Nomos Verlagsgesellschaft mbH 2018)

Willig C, *Introducing Qualitative Research in Psychology* (2 edn, McGraw-Hill Education 2008)

Smaranda Bara and Others v Casa Naţională de Asigurări de Sănătate and Others, Case C-201/14, [2015] (ECLI:EU:C:2015:638)

Facebook Ireland Ltd vs Maximillian Schrems (Schrems 2), Case C-311/18, [2020] (ECLI:EU:C:2020:559)

Maximillian Schrems v Data Protection Commissioner (Schrems), Case C-362/14, [2015] (ECLI:EU:C:2015:650)

European Commission v Republic of Austria, Case C-614/10, [2012] (ECLI:EU:C:2012:631)

Ker-Optika, Case C-108/09, [2015] (ECLI:EU:C:2010:725)

Productores de Música de España (Promusicae) v Telefónica de España SAU, Case C-275/06, [2008] (ECLI:EU:C:2008:54)

Árpád Kásler v OTP Jelzálogbank Zrt, Case C-26/13, [2014] (ECLI:EU:C:2014:282)

Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, [2015] (ECLI:EU:C:2014:317)

James Elliott Construction Limited v Irish Asphalt Limited, Case C-613/14, [2016] (ECLI:EU:C:2016:821)

Castelluccia C and others, 'Enhancing Transparency and Consent in the IoT' (IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, April 2018)

Crabtree A and Mortier R, ‘Human Data Interaction: Historical Lessons from Social Studies and CSCW’ (ECSCW 2015: Proceedings of the 14th European Conference on Computer Supported Cooperative Work, Oslo, 2015)

Hansen M, ‘Data Protection by Default in Identity-Related Applications’ (Policies and Research in Identity Management, Third IFIP WG 116 Working Conference, IDMAN 2013, London, April 2013)

Kamara I, Sveinsdottir T and Wurster S, ‘Raising Trust in Security Products and Systems through Standardisation and Certification: The Crisp Approach’ (ITU Kaleidoscope: Trust in the Information Society (K-2015), Barcelona, December 2015)

Mavroudis V and Veale M, ‘Eavesdropping Whilst You're Shopping: Balancing Personalisation and Privacy in Connected Retail Spaces’ (Proceedings of Living in the Internet of Things: Cybersecurity of the IoT, London, 2018)

Nouwens M and others, ‘Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence’ (CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, April 2020)

Ren J and others, ‘Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach’ (IMC '19: Proceedings of the Internet Measurement Conference, Amsterdam, October 2019)

Rossi A and Palmirani M, ‘A Visualization Approach for Adaptive Consent in the European Data Protection Framework’ (International Conference for E-Democracy and Open Government, Krems, May 2017)

Tran-Van P, Anciaux N and Pucheral P, ‘SWYSWYK: A Privacy-by-Design Paradigm for Personal Information Management Systems’ (International Conference on Information Systems Development(ISD), Cyprus, September 2017)

Varghese B and others, ‘Challenges and Opportunities in Edge Computing’ (IEEE International Conference on Smart Cloud (SmartCloud), New York, November 2016)

Bus J and Nguyen CM-H, ‘Personal Data Management a Structured Discussion’ in Hildebrandt M, O'Hara K and Waidner M (eds), *DigEnlight Yearbook: The Value of Personal Data* (Digital Enlightment 2013)

Carminati B, Ferrari E and Perego A, ‘Rule-Based Access Control for Social Networks’ in LNCS S (ed), *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops* (Springer Berlin Heidelberg 2006) <https://dx.doi.org/10.1007/11915072_80>

Chen J and others, ‘Who is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption’ 10 International Data Privacy Law 279

Chen J and Urquhart L, ‘On the Principle of Accountability: Challenges for Smart Homes and Cybersecurity’ in Crabtree A, Hamed H and Richard M (eds), *Privacy by Design for the Internet of Things: Building Accountability and Security* (IET 2021)

Hansen M, ‘Data Protection by Design and by Default à la European General Data Protection Regulation’ in Lehmann A and others (eds), *Privacy and Identity Management Facing up to Next Steps* (Springer International Publishing 2016)

Matzner T and others, ‘Do-It-Yourself Data Protection - Empowerment or Burden?’ in Gutwirth S, Ronald L and De Hert P (eds), *Data Protection on the Move Law, Governance and Technology Series*, vol 24 (Springer, Dordrecht 2016)

Milkaite I and Lievens E, ‘The Internet of Toys: Playing Games with Children's Data?’ in Mascheroni G and Holloway D (eds), *The Internet of Toys: Practices, Affordances and the Political Economy of Children's Play* (Palgrave Macmillan 2019)

Mohan J, Wasserman M and Chidambaram V, ‘Analyzing GDPR Compliance Through the Lens of Privacy Policy’ in Gadepally V and others (eds), *Heterogeneous Data Management, Polystores, and Analytics for Healthcare* (Springer International Publishing 2019)

Parker C, ‘Meta-regulation: Legal Accountability for Corporate Social Responsibility’ in McBarnet D, Voiculescu A and Campbell T (eds), *The New Corporate Accountability: Corporate Social Responsibility and the Law*, vol 29 (CUP 2007)

Prins C, ‘Property and Privacy : European Perspectives and the Commodification of our Identity’ in Guibault L and Hugenholtz BP (eds), *The Future of the Public Domain, Identifying the Commons in Information Law* (Kluwer Law International 2006)

Timmer A, ‘Vulnerability: Reflections on a New Ethical Foundation for Law and Politics’ in Fineman MA and Grear A (eds), *A Quiet Revolution: Vulnerability in the European Court of Human Rights* (Ashgate 2013)

Wright D and others, ‘Precaution and Privacy Impact Assessment as Modes Towards Risk Governance’ in von Schomberg R (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Field* (European Commission 2011)

Abiteboul S and Stoyanovich J, ‘Transparency, Fairness, Data Protection, Neutrality’ (2019) 11(3) Journal of Data and Information Quality 1

Adams A and Sasse MA, ‘Users are Not the Enemy’ (1999) 42(12) Commun Acm 40

Anciaux N and others, ‘Personal Data Management Systems: The Security and Functionality Standpoint’ (2019) 80 Information Systems 13

Arends J and others, ‘Multimodal Nocturnal Seizure Detection in a Residential Care Setting: A Long-Term Prospective Trial’ (2018) 91(21) Neurology e2010

Arnardóttir OM, ‘Vulnerability under Article 14 of the European Convention on Human Rights’ (2017) 1(3) Oslo Law Review 150

Bessant C, ‘Sharenting: Balancing the Conflicting Rights of Parents and Children’ (2018) 23(1) Communications Law 7

Binns R, ‘Data Protection Impact Assessments: a Meta-Regulatory Approach’ (2017) 7(1) International Data Privacy Law 22

Borenstein N and Blake J, ‘Cloud Computing Standards: Where's the Beef?’ (2011) 15(3) Ieee Internet Comput 74

Borgesius FZ, Helberger N and Reyna A, ‘The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law’ (2017) 54(5) Common Mkt Law Rev 1427

Brandimarte L, Acquisti A and Loewenstein G, ‘Misplaced Confidences’ (2013) 4(3) Social Psychological and Personality Science 340

Braun V and Clarke V, ‘Using Thematic Analysis in Psychology’ (2016) 3(2) Qualitative Research in Psychology 77

——, ‘Conceptual and Design Thinking for Thematic Analysis ’ (2021) 9(1) Qualitative Psychology 3

——, ‘One Size Fits All? What Counts as Quality Practice in (Reflexive) Thematic Analysis?’ (2021) 18(3) Qualitative Research in Psychology 328

——, ‘To Saturate or not to Saturate? Questioning Data Saturation as a Useful Concept for Thematic Analysis and Sample-Size Rationales’ (2021) 13(2) Qualitative Research in Sport, Exercise and Health 201

Buitelaar JC, 'Child's Best Interest and Informational Self-Determination: What the GDPR can Learn from Children's Rights' (2018) 8(4) International Data Privacy Law 293

Butterworth M, 'The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework' (2018) 34(2) Computer Law & Security Review 257

Buyya R and others, 'Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility' (2009) 25(6) Future Generation Computer Systems 599

Bygrave LA, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4(2) Oslo Law Review 105

Calo R, 'Privacy, Vulnerability, and Affordance' (2017) 66(2) The De Paul Law Review 591

Carolan E, 'The Continuing Problems with Online Consent under the EU's Emerging Data Protection Principles' (2016) 32(3) Computer Law & Security Review 462

Chamberlain A and others, 'Special Theme on Privacy and the Internet of Things' (2018) 22(2) Pers Ubiquit Comput 289

Chaudhry A and others, 'Personal Data: Thinking Inside the Box' (2015) 1(1) Aarhus Series on Human Centered Computing 4

Chen J and Urquhart L, '"They're all about pushing the products and shiny things rather than fundamental security": Mapping socio-technical challenges in securing the smart home' (2022) 31(1) Information & Communications Technology Law 99

Clarke V and Braun V, 'Thematic Analysis' (2017) 12(3) The Journal of Positive Psychology 297

Clifford D and Ausloos J, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130

——, 'Data Protection and the Role of Fairness' 37 Yearbook of European Law 130

Cohen JE, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52(5) Stanford Law Review 1373

Collingwood L, 'Villain or Guardian? 'The Smart Toy is Watching You Now … .'' 30(1) Information & Communications Technology Law 75

Cooper FR, 'Always Already Suspect: Revising Vulnerability Theory' (2015) 93(5) North Carolina Law Review 1339

Crabtree A and others, 'Building Accountability into the Internet of Things: the IoT Databox Model' (2018) 4(1) Journal of Reliable Intelligent Environments 39

Custers B and others, 'A Comparison of Data Protection Legislation and Policies Across the EU' (2018) 34(2) Computer Law & Security Review 234

D'Cruz H, Gillingham P and Melendez S, 'Reflexivity, its Meanings and Relevance for Social Work: A Critical Review of the Literature' (2005) 37(1) Brit J Soc Work 73

Demetzou K, 'Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of 'High Risk' in the General Data Protection Regulation' (2019) 35(6) Computer Law & Security Review 105342

Di Martino B and others, 'Internet of Things Reference Architectures, Security and Interoperability: A Survey' (2018) 1(2) Internet of Things 99

Diaz C, Tene O and Gurses S, 'Hero or Villain: the Data Controller in Privacy Law and Technologies' (2013) 74(6) Ohio State Law Journal 923

Ferretti F, ‘Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?’ (2014) 51(3) Common Mkt Law Rev 843

Fineman MA, ‘The Vulnerable Subject: Anchoring Equality in the Human Condition’ (2008) 20(1) Yale Journal of Law and Feminism 1

Garber J, ‘GDPR – Compliance Nightmare or Business Opportunity?’ (2018) 2018(6) Computer Fraud & Security 14

Gleeson NC and Walden I, ‘'It's a Jungle Out There'?: Cloud Computing, Standards and the Law’ (2014) 5(2) European Journal of Law and Technology

Gonçalves ME, ‘The Risk-Based Approach Under the New EU Data Protection Regulation: a Critical Perspective’ (2020) 23(2) Journal of Risk Research 139

Graef I, Clifford D and Valcke P, ‘Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law’ (2018) 8(3) International Data Privacy Law 200

Gürses S, ‘PETs and their Users: a Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm’ (2010) 3(3) Identity in the Information Society 539

Hadar I and others, ‘Privacy by Designers: Software Developers’ Privacy Mindset’ (2018) 23(1) Empirical Software Engineering 259

——, ‘Privacy by Designers: Software Developers’ Privacy Mindset’ [Springer Science and Business Media LLC] 23 Empirical Software Engineering 259

Hall MA, ‘Property, Privacy and the Pursuit of Integrated Electronic Medical Records’ (2014) ssrn: 1334963 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=133496> accessed 1 July 2022

Hildebrandt M, ‘Profiling and the Rule of Law’ (2008) 1(1) Identity in the Information Society 55

——, ‘Balance or Trade-off? Online Security Technologies and Fundamental Rights’ (2013) 26(4) Philosophy & Technology 357

Hildebrandt M and Koops B-J, ‘The Challenges of Ambient Law and Legal Protection in the Profiling Era’ (2010) 73(3) Modern Law Review 428

Hildebrandt M and Tielemans L, ‘Data Protection by Design and Technology Neutral Law’ (2013) 29(5) Computer Law & Security Review 509

Hon WK, Millard C and Walden I, ‘The Problem of ‘Personal Data' in Cloud Computing: what Information is Regulated? - the Cloud of Unknowing’ (2011) 1(4) International Data Privacy Law 211

Hutchinson T and Duncan N, ‘Defining and Describing What We Do: Doctrinal Legal Research’ (2012) 17(1) Deakin Law Review 83

Iafrati R, ‘Can the CCPA Access Right Be Saved? Realigning Incentives in Access Request Verification’ (2020) 20(1) Pittsburgh Journal of Technology Law & Policy

Irion K and Helberger N, ‘Smart TV and the Online Media Sector: User Privacy in View of Changing Market Realities’ (2017) 41(3) Telecommunications Policy 170

Janeček V, ‘Ownership of Personal Data in the Internet of Things’ (2018) 34(5) Computer Law & Security Review 1039

Janssen H and others, ‘Decentralized Data Processing: Personal Data Stores and the GDPR’ (2021) 10(4) International Data Privacy Law 356

Johnson SD and others, ‘The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay’ (2020) 15(1) PLOS ONE 1

Kang J and Buchner B, ‘Privacy in Atlantis’ (2004) 18(1) Harvard Journal of Law & Technology 229

Kish LJ and Topol EJ, ‘Unpatients - Why Patients Should Own their Medical Data’ (2015) 33(9) Nature Biotechnology 921

Lee J, ‘A View Of Cloud Computing’ (2013) 1(1) International Journal of Networked and Distributed Computing 2

Lenaerts K, ‘Limits on Limitations: The Essence of Fundamental Rights in the EU’ (2019) 20(6) German Law Journal 779

Lessig L, ‘Privacy as Property’ (2002) 69(1) Social Research: An International Quarterly of Social Sciences 247

Li Z, Sharma V and Mohanty SP, ‘Preserving Data Privacy via Federated Learning: Challenges and Solutions’ (2020) 9(3) Ieee Consum Electr M 8

Lievens E and Hof Svd, ‘The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR’ (2018) Communications Law 33

Litman J, ‘Information Privacy/Information Property’ (2000) 52(5) Stanford Law Review 1283

Livingstone S, ‘Children: a Special Case for Privacy?’ (2018) 46(2) Intermedia 18

Luna F, ‘Elucidating the Concept of Vulnerability: Layers Not Labels’ (2009) 2(1) International Journal of Feminist Approaches to Bioethics 121

Lupton D and Williamson B, ‘The Datafied Child: The Dataveillance of Children and Implications for their Rights’ (2017) 19(5) New Media & Society 780

Macenaite M, ‘From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation’ (2017) 19(5) New Media & Society 765

Macenaite M and Kosta E, ‘Consent for Processing Children’s Personal Data in the EU: Following in US footsteps?’ (2017) 26(2) Information & Communications Technology Law 146

Malgieri G and Niklas J, ‘Vulnerable Data Subjects’ (2020) 37 Computer Law & Security Review 105415

Mantelero A, ‘AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment’ (2018) 34(4) Computer Law & Security Review 754

Manwaring K, ‘Emerging Information Technologies: Challenges for Consumers’ (2017) 17(2) Oxford University Commonwealth Law Journal 265

Marwick AE and Boyd D, ‘Networked Privacy: How Teenagers Negotiate Context in Social Media’ (2014) 16(7) New Media & Society 1051

Micheti A, Burkell J and Steeves V, ‘Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand’ (2010) 30(2) Bulletin of Science, Technology & Society 130

Milkaite I and Lievens E, ‘Child-Friendly Transparency of Data Processing in the EU: from Legal Requirements to Platform Policies’ (2019) 14(1) Journal of Children and Media 5

Mocrii D, Chen Y and Musilek P, ‘IoT-Based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security’ (2018) 1-2 Internet of Things 81

Moerel L and Prins C, ‘Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things’ ssrn: 2784123 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123> accessed 1 July 2022

Montgomery KC, ‘Youth and Surveillance in the Facebook Era: Policy Interventions and Social Implications’ (2015) 39(9) Telecommunications Policy 771

Morey T, Forbath T and Schoop A, ‘Customer Data: Designing for Transparency and Trust’ (2015) 93(5) Harvard Business Review 96

Myers MD and Newman M, ‘The Qualitative Interview in IS Research: Examining the Craft’ (2007) 17(1) Information and Organization 2

Ni Loideain N, ‘A Port in the Data-Sharing Storm: the GDPR and the Internet of Things’ (2019) 4(2) Journal of Cyber Policy 178

Ni Loideain N, Adams R and Clifford D, ‘Gender as Emotive AI and the Case of ‘Nadia’: Regulatory and Ethical Implications’ SSRN Electronic Journal ssrn: 3858431 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3858431> accessed 1 July 2022

Noto La Diega G and Sappa C, ‘The Internet of Things (IoT) at the Intersection of Data Protection and Trade Secrets. Non-Conventional Paths to Counter Data Sppropriation and Empower Consumers’ (2020) 3 European Journal of Consumer Law 419

Noto La Diega G and Walden I, ‘Contracting for the 'Internet of Things': Looking into the Nest’ (2016) 7(2) European Journal of Law and Technology 1

Ohm P, ‘Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization’ (2010) 57(6) UCLA Law Review 1701

Orlikowski WJ, ‘Sociomaterial Practices: Exploring Technology at Work’ (2007) 28(9) Organization Studies 1435

Pamela S, ‘Privacy as Intellectual Property?’ (2000) 52(5) Stanford Law Review 1125

Palmdorf S and others, ‘Technology-Assisted Home Care for People With Dementia and Their Relatives: Scoping Review’ (2021) 4(1) JMIR Aging e25307

Peppet SR, ‘Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent’ (2014) 93(1) Texas Law Review 85

Perera CA and others, ‘Valorising the IoT Databox: Creating Value for Everyone’ (2016) 28(1) Trans Emerging Telecommunications Technologies 1

Peroni L and Timmer A, ‘Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention law’ (2013) 11(4) International Journal of Constitutional Law 1056

Piasecki S, Urquhart L and McAuley D, ‘Defence Against the Dark Artefacts: Smart Home Cybercrimes and Cybersecurity Standards’ (2021) 42 Computer Law & Security Review 105542

Purtova N, ‘Do Property Rights in Personal Data Make Sense after the Big Data Turn?: Individual Control and Transparency’ (2017) 10(2) Journal of Law and Economic Regulation 64

Raab CD, ‘Information Privacy, Impact Assessment, and the Place of Ethics’ (2020) Computer Law & Security Review 105404

Reidenberg JR, ‘Lex Informatica: The Formulation of Information Policy Rules through Technology’ (1997) 76(3) Texas Law Review 553

Roman R, Najera P and Lopez J, ‘Securing the Internet of Things’ (2011) 44(9) Computer 51

Romanou A, ‘The Necessity of the Implementation of Privacy by Design in Sectors where Data Protection Concerns Arise’ (2018) 34(1) Computer Law & Security Review 99

Solove DJ, ‘Identity Theft, Privacy, and the Architecture of Vulnerability’ (2003) 54(4) The Hastings Law Journal 1227

—–, ‘Introduction: Privacy Self-Management and the Consent Dilemma’ (2013) 126(7) Harvard Law Rev 1880

Sutherland RJ and Isherwood T, ‘The Evidence for Easy-Read for People With Intellectual Disabilities: A Systematic Literature Review’ (2016) 13(4) Journal of Policy and Practice in Intellectual Disabilities 297

Tikkinen-Piri C, Rohunen A and Markkula J, ‘EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies’ (2018) 34(1) Computer Law & Security Review 134

Troncoso C and others, ‘Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments’ (2017) 4 Proceedings on Privacy Enhancing Technologies, De Gruyter Open 307

Urquhart L, Crabtree A and Lodge T, ‘Demonstrably Doing Accountability in the Internet of Things’ (2018) 27(1) International Journal of Law and Information Technology 1

Urquhart L, Sailaja N and McAuley D, ‘Realising the Right to Data Portability for the Domestic Internet of Things’ (2018) 22(2) Pers Ubiquit Comput 317

Urquhart L, Schnädelbach H and Jäger N, ‘Adaptive Architecture: Regulating Human Building Interaction’ (2019) 33(1) International Review of Law, Computers & Technology 3

van der Hof S, ‘I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World’ (2016) 34(2) Wisconsin International Law Journal 409

Van Dijk N, Gellert R and Rommetveit K, ‘A Risk to a Right? Beyond Data Protection Risk Assessments’ (2016) 32(2) Computer Law & Security Review 286

Varghese B, ‘A History of the Cloud’ (2019) 61(2) ITNOW 46

Varghese B and Buyya R, ‘Next Generation Cloud Computing: New Trends and Research Directions’ (2018) 79(3) Future Generation Computer Systems 849

Veale M, Binns R and Ausloos J, ‘When Data Protection by Design and Data Subject Rights Clash’ (2018) 8(2) International Data Privacy Law 105

Volosevici D, ‘Child Protection under GDPR’ (2019) 6(2) A Journal of Social and Legal Studies 17

Wachter S, ‘Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR’ (2017) 34(3) Computer Law & Security Report 436

—–, ‘The GDPR and the Internet of Things: A Three-Step Transparency Model’ (2018) 10(2) Law, Innovation and Technology 266

Walsham G, ‘Doing Interpretive Research’ (2006) 15(4) European Journal of Information Systems 320

Wiese Schartum D, ‘Making Privacy by Design Operative’ (2016) 24(2) International Journal of Law and Information Technology 151

Zeadally S and others, ‘Smart Healthcare: Challenges and Potential Solutions Using Internet of Things (IoT) and Big Data Analytics’ (2020) 4(2) PSU Research Review 93

Convention on the Rights of Persons with Disabilities GA Res. 61/106, annex, 61 UN Gaor supp. (No 49) at 65, UN doc. A/61/49 (2006)

Convention on the Rights of the Child, GA Res. 44/25, annex, 44 UN GAOR Supp. (No 49) at 167, UN Doc. A/44/49 (1989)

Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts [1993] OJ L 95/29

Convention on the International Protection of Adults, The Hague, UN, Treaty Series, vol. 2600, at 3 (2000)

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market [2000] OJ L 178

Directive (EU) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [2002] OJ L 201/37

Safeguarding Vulnerable Groups Act 2006

Charter of Fundamental Rights of the European Union [2012] OJ C 326

Regulation (EU) 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, [2021] OJ L 316/12

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L 241

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive, ‘LED’), [2016] OJ L119

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation, ‘GDPR’), [2016] OJ L 119/1

European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2017/0003’ (COD), Brussels, COM (2017) 10 final

Data Protection Act 2018 (UK)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Heuvel Kvd, ‘Securing the Smart Home’ (Masters thesis, University of Amsterdam 2018)

Timmer A, ‘Strengthening the Equality Analysis of the European Court of Human Rights: The Potential of the Concepts of Stereotyping and Vulnerability’ (Doctor of Law, Universiteit Gent 2014)

Urquhart L, ‘Towards User Centric Regulation: Exploring the Interface Between Information Technology Law and Human Computer Interaction’ (DPhil, University of Nottingham 2017)

Activinsights, ‘Activinsights Band’ (2021) <https://www.activinsights.com/products/activinsights-band/> accessed 1 July 2022

Antipolis S, ‘ETSI Releases First Globally Applicable Standard for Consumer IoT Security ’ (*ETSI*, 19 February 2019) <https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security> accessed 1 July 2022

Armbrust M and others, ‘Above the Clouds: A Berkeley View of Cloud Computing’ (*University of California, Berkeley*, 2009) <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html> accessed 1 July 2022

Arnold B and Sivasothy K, ‘He Sees You when You’re Sleeping, He Knows When You’re Awake: Smart Toys and Regulating the IoT in Canada’ (*Gowling WLG*, 17 December 2018) <https://gowlingwlg.com/en/insights-resources/articles/2018/smart-toys-and-regulating-the-iot-in-canada/> accessed 1 July 2022

Article 29 Working Party, ‘The Future of Privacy. Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data’ (WP 168, 2009)

––, ‘Opinion 02/2013 on Apps on Smart Devices’ (WP 202, 2013)

––, ‘Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC ’ (WP 217, 2014)

––, ‘Opinion 8/2014 on the recent developments on the Internet of Things’ (WP 223, 16 September 2004)

––, ‘Guidelines on data protection impact assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679’ (WP 248, 4 October 2017)

––, ‘Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679’ (WP 251, 2018)

––, ‘Guidelines on Consent Under Regulation 2016/679’ (WP 259, 2018)

––, ‘Guidelines on Transparency under Regulation 2016/679’ (WP 260, 2017)

Baraniuk C, ‘Sensors and AI to monitor Dorset social care patients’ (*BBC*, 2021) <https://www.bbc.com/news/technology-58317106> accessed 1 July 2022

BCL Solicitors LLP, ‘£18.4 Million Marriot International GDPR Fine Announced by IPO: What Did we Learn?’ (2 December 2020) <https://www.lawyer-monthly.com/2020/11/18-4-million-marriott-international-gdpr-fine-announced-by-ipo-what-did-we-learn/> accessed 1 July 2022

Bits of Freedom, ‘A Loophole in Data Processing’ (11 December 2012) <https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf> accessed 1 July 2022

Bouvet on behalf of the Norwegian Consumer Council, ‘Investigation of Privacy and Security Issues with Smart Toys’ (2 November 2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf> accessed 1 July 2022

Bowles N, ‘Thermostats, Locks and Lights: Digital Tools of Domestic Abuse’ (*The New York Times*, 2018) <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html> accessed 1 July 2022

Brochot G and others, ‘Study on Personal Data Stores conducted at the Cambridge University Judge Business School’ (*European Commission*, 7 August 2015) < https://digital-strategy.ec.europa.eu/en/library/study-personal-data-stores-conducted-cambridge-university-judge-business-school> accessed 1 July 2022

BSI, ‘BSI Launches Kitemark for Internet of Things Devices’ (15 May 2018) <https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/may/bsi-launches-kitemark-for-internet-of-things-devices/> accessed 1 July 2022

——, ‘BSI Kitemark for Products’ (2019) <https://www.bsigroup.com/en-GB/kitemark/product-testing/> accessed 1 July 2022

——, ‘Standards and Regulation’ (2021) <https://www.bsigroup.com/en-GB/standards/Information-about-standards/standards-and-regulation/> accessed 1 July 2022

Burgess PJ and others, ‘Towards a Digital Ethics’ (*EDPS Ethics Advisory Group*, 2018) <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf> accessed 1 July 2022

Centre for Information Policy Leadership, ‘GDPR Implementation in Respect of Children’s Data and Consent’ (5 March 2018) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf> accessed 1 July 2022

Cimpanu C, ‘Alexa and Google Home Devices Leveraged to Phish and Eavesdrop on Users, Again’ (*ZDNet*, 20 October 2019) <https://www.zdnet.com/article/alexa-and-google-home-devices-leveraged-to-phish-and-eavesdrop-on-users-again/> accessed 1 July 2022

CitizenMe, ‘Global Collaborative Intelligence with ZeroData’ (2021) <https://www.citizenme.com/> accessed 1 July 2022

CloudLocker, ‘CloudLocker’ (2021) < https://www.cloudlocker.io/> accessed 1 July 2022

Cruz Villalón P, ‘Opinion of Advocate General Cruz Villalón Pedro delivered on 9 July 2015, Case C-201/14, Smaranda Bara and Others,’ (9 July 2015) <https://curia.europa.eu/juris/document/document.jsf?docid=165642&doclang=en> accessed 1 July 2022

CSA, ‘Building the Foundation and Future of the IoT’ (*CSA*, 2022) <https://csa-iot.org/> accessed 1 July 2022

——, ‘Matter, The Foundation for Connected Things’ (*CSA*, 2022) <https://csa-iot.org/all-solutions/matter/> accessed 1 July 2022

Data Protection Commission, ‘Data Protection Commission’s two statutory inquiries into Facebook’s processing of children’s data on Instagram (opened in Sept 2020)’ (19 October 2020) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commissions-two-statutory-inquiries-facebooks-processing-childrens-data-instagram> accessed 1 July 2022

Day M and Drozdiak N, ‘Thousands of Amazon Workers Listen to Alexa Users' Conversations’ (*Time*, 11 April 2019) <https://time.com/5568815/amazon-workers-listen-to-alexa/> accessed 1 July 2022

DCMS, ‘Consultation on the Government's Regulatory Proposals regarding Consumer Internet of Things (IoT) Security’ (3 February 2020) <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security> accessed 1 July 2022

——, ‘Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report’ (2018) <https://www.gov.uk/government/publications/secure-by-design-report> accessed 1 July 2022

——, ‘Code of Practice for Consumer IoT Security’ (October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf> accessed 1 July 2022

——, ‘Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security’ (October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/774438/Map

ping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf> accessed 1 July 2022

digi.mi, 'What is digi.me?' (2021) <https://digi.me/what-is-digime/> accessed 1 July 2022

Donoso V, Van Mechelen M and Verdoodt V, 'Increasing User Empowerment through Participatory and Co-design Methodologies' (*EMSOC*, 2014) <https://www.researchgate.net/publication/298722734_Increasing_User_Empowerment_through_Participatory_and_Co-design_Methodologies_EMSOC_report> accessed 1 July 2022

EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (12-13 November 2019) <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf> accessed 1 July 2022

——, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (16 October 2019) <https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_en> accessed 1 July 2022

——, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 1 July 2022

EDPS, 'Personal Information Management Systems' (6 January 2021) <https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-32020-personal-information_en> accessed 1 July 2022

——, 'European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the Data Protection Reform Package' (7 March 2012) <https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf> accessed 1 July 2022

——, 'Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (11 April 2017) <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf> accessed 1 July 2022

——, 'Opinion 4/2015 Towards a New Digital Ethics' (11 September 2015) <https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf> accessed 1 July 2022

——, 'EDPS Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data' (19 December 2019) <https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf> accessed 1 July 2022

——, 'Opinion 9/2016 on Personal Information Management Systems' (20 October 2016) <https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en> accessed 1 July 2022

Eindhoven University of Technology, 'New Epilepsy Warning Device Could Save Thousands of Lives' (26 October 2018) <https://www.tue.nl/en/news/news-overview/24-10-2018-new-epilepsy-warning-device-could-save-thousands-of-lives/#top> accessed 1 July 2022

ENISA, 'IoT Security Standards Gap Analysis' (17 January 2019) <https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis> accessed 1 July 2022

——, 'Security Certification Practice in the EU' (21 November 2013) <https://www.enisa.europa.eu/publications/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study> accessed 1 July 2022

——, 'Recommendations on Shaping Technology According to GDPR Provisions - Exploring the Notion of Data Protection by Default' (28 January 2018) <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2> accessed 1 July 2022

——, 'Reinforcing Trust and Security in the Area of Electronic Communications and Online Services. Sketching the Notion of 'State-of-the-Art' for SMEs in Security of Personal Data Processing' (28 January 2019) <https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-in-the-area-of-electronic-communications-and-online-services> accessed 1 July 2022

Erickson A, 'This Pretty Blond Doll Could be Spying on your Family' (2017) <https://www.washingtonpost.com/news/worldviews/wp/2017/02/23/this-pretty-blond-doll-could-be-spying-on-your-family/?noredirect=on&utm_term=.00adeafac872> accessed 1 July 2022

Ethyca CK, 'Twitter and Microsoft show Data Privacy is Moving from Sticking Point to Selling Point' (*VB*, 21 December 2019) <https://venturebeat.com/2019/12/21/twitter-and-microsoft-show-data-privacy-is-moving-from-sticking-point-to-selling-point/> accessed 1 July 2022

ETSI, 'EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements' (June 2020) <https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf> accessed 1 July 2022

European Commission, 'Methods of Referencing Standards in Legislation with an Emphasis on European Legislation' (2002) <https://ec.europa.eu/docsroom/documents/3276/attachments/1/translations/en/renditions/native> accessed 1 July 2022

——, 'How to Write Clearly' (*europa.eu*, 2011) <https://op.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5> accessed 1 July 2022

——, 'Harmonised Standards' (2019) <https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en> accessed 1 July 2022

European Commission CftCttEP, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020)710 final, 'A European Strategy for Data' (*European Commission*, 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN> accessed 1 July 2022

EUSoft, 'We are ISO 27001 Certified!' (28 March 2019) <https://www.eusoft.co.uk/we-are-iso-27001-certified/> accessed 1 July 2022

Financial Times, 'Living with the Cost of Dementia' (2021) <https://www.ft.com/content/4baeeb4e-d680-11e6-944b-e7eb37a6aa8e> accessed 1 July 2022

Forbrukerradet (Norwegian Consumer Council), '#Toyfail An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys' (December 2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf> accessed 1 July 2022

Foxglove, 'YouTube Data Breach Claim' (14 September 2020) <https://www.foxglove.org.uk/2020/09/14/youtube-is-breaking-the-law-by-harvesting-childrens-data-for-targeted-advertising-our-work-to-stop-them/> accessed 1 July 2022

FRA, 'Handbook on European Data Protection Law' (April 2018) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf> accessed 1 July 2022

Gartner, 'Leading the IoT: Gartner Insights on How to Lead in a Connected World' (2017) <https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf> accessed 1 July 2022

Gibbs S, 'Hackers can Hijack Wi-Fi Hello Barbie to Spy on your Children' (*The Guardian*, 26 November 2015) <https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children> accessed 1 July 2022

Google, 'Technologies' (2021) <https://policies.google.com/technologies/partner-sites?hl=en-US> accessed 1 July 2022

Gruman G, 'IoT Silliness: 'Headless' devices without a UI' (*InfoWorld*, 13 January 2015) <https://www.infoworld.com/article/2867356/beware-this-iot-fallacy-the-headless-device.html> accessed 1 July 2022

Guardian T, 'High-Tech Epilepsy Warning Device Could Save Lives' (11 January 2019) <https://guardian.ng/features/health/high-tech-epilepsy-warning-device-could-save-lives-2/> accessed 1 July 2022

ID Cyber Solutions, 'Cyber Essentials Plus' (2022) <https://cyberessentials.online/cyber-essentials-plus/> accessed 1 July 2022

IEEE, 'Towards a Definition of the Internet of Things (IoT)' (27 May 2015) <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf> accessed 1 July 2022

Information Commissioner's Office, 'Age Appropriate Design: a Code of Practice for Online Services' (2 September 2021) <https://ico.org.uk/for-organisations/childrens-code-hub/> accessed 1 July 2022

——, 'Big Data, Artificial Intelligence, Machine Learning and Data Protection' (9 September 2017) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 1 July 2022

——, 'ICO Fines British Airways £20m for Data Breach Affecting more than 400,000 Customers' (16 October 2020) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/> accessed 1 July 2022

——, 'Update Report into Adtech and Real Time Bidding' (20 June 2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf> accessed 1 July 2022

——, 'ICO Codes of Conduct and Certification Schemes Open for Business' (28 February 2020) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/02/ico-codes-of-conduct-and-certification-schemes-open-for-business/> accessed 1 July 2022

——, 'Guide to the General Data Protection Regulation (GDPR)' (2018) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> accessed 1 July 2022

——, 'Children' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/> accessed 1 July 2022

——, 'Contract' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/> accessed 1 July 2022

——, 'Data Protection by Design and Default' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> accessed 1 July 2022

——, 'Lawful Basis for Processing' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> accessed 1 July 2022

——, 'Legitimate Interests' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/> accessed 1 July 2022

——, 'Principle (c): Data minimisation ' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> accessed 1 July 2022

——, 'Right to be Informed' (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/> accessed 1 July 2022

——, ‘Special Category Data’ (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/> accessed 1 July 2022

——, ‘Vital Interests’ (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/> accessed 1 July 2022

——, ‘What is a DPIA?’ (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/> accessed 1 July 2022

——, ‘When do we need to do a DPIA?’ (2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/> accessed 1 July 2022

——, ‘The UK GDPR’ (2022) <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/> accessed 1 July 2022

Ingrida M and others, ‘The General Data Protection Regulation and Children’s Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society. Roundtable Report’ (*Ghent University*, 2017) <https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf> accessed 1 July 2022

IRMA, ‘IRMA in Detail’ (2021) <https://privacybydesign.foundation/irma-explanation/> accessed 1 July 2022

ISO, ‘BS ISO/IEC 29184 Information Technology - Online Privacy Notices and Consent’ (2018) <https://standardsdevelopment.bsigroup.com/projects/2016-01083> accessed 1 July 2022

——, ‘ISO/PC 317 Consumer Protection: Privacy by Design for Consumer Goods and Services ’ (2018) <https://www.iso.org/committee/6935430.html> accessed 1 July 2022

——, ‘ISO/IEC 27701:2019 Security Techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management - Requirements and Guidelines’ (August 2019) <https://www.iso.org/standard/71670.html> accessed 1 July 2022

Kelion L, ‘Amazon Sued over Alexa Child Recordings in US’ (*BBC*, 13 June 2019) <https://www.bbc.com/news/technology-48623914> accessed 1 July 2022

Lewkowicz J, ‘Apple shows off new security features, iOS 13 and new iPad OS at WWDC’ (*SD Times*, 3 June 2019) <https://sdtimes.com/softwaredev/apple-shows-off-new-security-features-ios-13-and-new-ipad-os-at-wwdc/> accessed 1 July 2022

Livingstone S and Haddon L, ‘EU Kids Online’ (2009) <http://eprints.lse.ac.uk/24372/1/EU%20Kids%20Online%20final%20report%202009%28lsero%29.pdf> accessed 1 July 2022

Lomas N, ‘YouTube Hit with UK Class Action Style Suit Seeking $3BN+ for ‘Unlawful’ Use of Kids’ Data’ (*TechCrunch+*, 14 September 2020) <https://techcrunch.com/2020/09/14/youtube-hit-with-uk-class-action-style-suit-seeking-3bn-for-unlawful-use-of-kids-data/> accessed 1 July 2022

Lueth KL, ‘State of the IoT 2018: Number of IoT Devices now at 7B – Market Accelerating’ (*IoT Analytics,*, 8 August 2018) <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/> accessed 1 July 2022

Martin C, ‘Personal Data: French Data Protection Authority Levies €50 Million Fine (Ogletree Deakins, 18 February 2019) <https://ogletree.com/insights/personal-data-french-data-protection-authority-levies-e50-million-fine/> accessed 1 July 2022

McCann D and others, ‘YouTube Data Breach Claim’ (2022) <https://www.youtubedataclaim.co.uk/> accessed 1 July 2022

midata, ‘My Data – Our Health’ (2021) <https://www.midata.coop/en/home/> accessed 1 July 2022

Mondaq, ‘ICO Imposes Maximum pre-GDPR Fine on Major UK Retailer: Cybersecurity Lessons for Retailers (and other Organisations)’ (19 February 2020) <https://www.dentons.com/en/insights/articles/2020/february/10/ico-imposes-maximum-pre-gdpr-fine-on-major-uk-retailer> accessed 1 July 2022

Mortier R and others, ‘Human-Data Interaction: The Human Face of the Data-Driven Society’ (*arXiv:1412.6159*, 6 January 2015) <https://arxiv.org/abs/1412.6159> accessed 1 July 2022

MyDex, ‘Mydex CIC Helps Individuals and Service Providers Improve their Handling of Personal Data’ (2021) <https://mydex.org/> accessed 1 July 2022

OECD, ‘OECD Policy Roundtable on Standard-Setting’ (2010) <http://www.oecd.org/daf/competition/47381304.pdf> accessed 1 July 2022

OpenPDS, ‘Philosophy’ (2021) <https://openpds.media.mit.edu/> accessed 1 July 2022

Osborne Clarke, ‘Consumer Data and the Complex World of Data Ownership’ (2015) <https://www.osborneclarke.com/insights/consumer-data-and-the-complex-world-of-data-ownership/> accessed 1 July 2022

Parliament U, ‘Edge Computing, Postnote 631’ (2020) <https://post.parliament.uk/research-briefings/post-pn-0631/> accessed 1 July 2022

Pullen JP, ‘Where Did Cloud Computing Come From, Anyway?’ (*Time*, 2015) <https://time.com/collection-post/3750915/cloud-computing-origin-story/> accessed 1 July 2022

Salm C, ‘Protection of Vulnerable Adults’ (*European Parliament, European Parliamentary Research Service*, September 2016) <https://www.europarl.europa.eu/RegData/etudes/STUD/2016/581388/EPRS_STU(2016)581388_EN.pdf> accessed 1 July 2022

Sanuj, ‘iOS 15: How to Use Siri Offline on iPhone and iPad (Without Internet)’ (*iGEEKSBLOG*, 9 June 2022) <https://www.igeeksblog.com/how-to-use-siri-offline-on-iphone-ipad/> accessed 1 July 2022

Silicon Labs, ‘CHIP 180 - Connected Home over IP’ (2022) <https://www.silabs.com/support/training/connected-home-over-ip-intro> accessed 1 July 2022

Solid, ‘What is Solid?’ (2020) <https://inrupt.com/solid/> accessed 1 July 2022

——, ‘Fully Interoperable Standards’ (2021) <https://solidproject.org/> accessed 1 July 2022

The Royal Society, ‘Protecting Privacy in Practice. The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis’ (March 2019) <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf> accessed 1 July 2022

TSA, ‘The Quality Standards Framework’ (2022) <https://www.tsa-voice.org.uk/-covid-19/safe-working-environments/quality-standards-fr/> accessed 1 July 2022

Tuohy J, ‘Matter Smart Home Standard Delayed Until Fall 2022’ (*The Verge*, 17 March 2022) <https://www.theverge.com/2022/3/17/22982166/matter-smart-home-standard-postponed-fall-2022> accessed 1 July 2022

Turner S, ‘Connected Toys: What Device Documentation Explains about Privacy and Security’ (*PETRAS*, 2020) <https://discovery.ucl.ac.uk/id/eprint/10100395/7/Turner_PETRAS_Connected-Toys_whitepaper_12062020.pdf> accessed 1 July 2022

UNICEF, ‘UN Convention on the Rights of the Child in Child Friendly Language 2016’ (2016) <https://www.unicef.org/sop/convention-rights-child-child-friendly-version> accessed 1 July 2022

Van Breda B and others, ‘Smart TV and Data Protection’ (*European Audiovisual Observatory*, 2016) <https://rm.coe.int/iris-special-2015-smart-tv-and-data-protection/1680945617> accessed 1 July 2022

Vectra, ‘Spotlight Report on Healthcare’ (2019) <https://www.vectra.ai/download/spotlight-report-on-healthcare-2019#form-download> accessed 1 July 2022

Williams A, ‘Smart Home Privacy: What Amazon, Google and Apple do with your Data’ (*The Ambient*, 2019) <https://www.the-ambient.com/features/how-amazon-google-apple-use-smart-speaker-data-338> accessed 1 July 2022

Wired, ‘Decentralised AI has the Potential to Upend the Online Economy’ (2021) <https://www.wired.co.uk/article/decentralised-artificial-intelligence> accessed 1 July 2022

Wituschek J, ‘96% of iPhone Users have Opted Out of App Tracking Since iOS 14.5 Launched’ (*iMore*, 6 May 2021) <https://www.imore.com/96-iphone-users-have-opted-out-app-tracking-ios-145-launched> accessed 1 July 2022