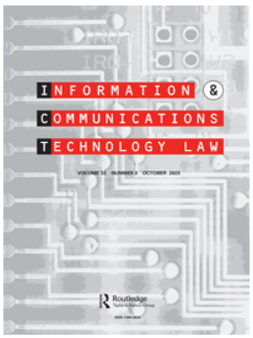

Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: (Print) (Online) Journal homepage: www.informahealthcare.com/journals/cict20

Expert perspectives on GDPR compliance in the context of smart homes and vulnerable persons

Stanislaw Piasecki

To cite this article: Stanislaw Piasecki (2023) Expert perspectives on GDPR compliance in the context of smart homes and vulnerable persons, Information & Communications Technology Law, 32:3, 385-417, DOI: 10.1080/13600834.2023.2231326

To link to this article: https://doi.org/10.1080/13600834.2023.2231326

Published online: 07 Jul 2023.

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW
2023, VOL. 32, NO. 3, 385–417
https://doi.org/10.1080/13600834.2023.2231326

Routledge
Taylor & Francis Group

Expert perspectives on GDPR compliance in the context of smart homes and vulnerable persons

Stanislaw Piasecki

Institute for Information Law, University of Amsterdam, Amsterdam, Netherlands

ABSTRACT

This article introduces information gathered through 21 semi-structured interviews conducted with UK, EU and international professionals in the field of General Data Protection Regulation (GDPR) compliance and technology design, with a focus on the smart home context and vulnerable people using smart products. Those discussions gave various insights and perspectives into how the two communities (lawyers and technologists) view intricate practical data protection challenges in this specific setting. The variety of interviewees allowed to compare different 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 challenges faced by organisations working on smart devices used by vulnerable persons? How do experts perceive data protection law-related problems in this context?

KEYWORDS

Smart devices; vulnerable people; IoT; GDPR; data protection; empirical

1. Introduction

This article analyses experiences, opinions and perceptions of 21 experts (through semi-structured interviews conducted by a single interviewer) concerning data protection law compliance issues when vulnerable people use smart home products.[1] The General Data Protection Regulation (GDPR) – a European Union law regulation related to data protection and privacy in the EU and the European Economic Area (adopted to increase individuals' control and rights in relation to their personal data) – contains several articles on vulnerability and organisations need to implement relevant provisions.[2] For example, Art. 6.1 (f) states that companies must be especially strict when balancing their own

CONTACT Stanislaw Piasecki s.piasecki@uva.nl

[1]This study was approved by the Research Ethics Committee of the School of Computer Science, University of Nottingham (reference: CS-2020-R11).

[2]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.

interests against those of a child. While there have been doctrinal efforts in this field, 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.[3] 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 (apart from provisions directly related to children, Rec. 75 of the GDPR mentions processing 'personal data of vulnerable natural persons, in particular of children' as particularly risky, placing emphasis on the latter while not excluding other vulnerable groups).[4] This means organisations need to adapt their data protection policies to children's and other vulnerable people's needs. How does GDPR compliance work in practice in the context of vulnerable people using smart home devices? How do professionals consider data protection-related issues?

This article focusses on smart homes not only for the reason that this is an increasingly prominent sector where numerous legal problems appear but also due to issues caused by the implementation of certain technical measures, which do not always reflect the requirements of our present-day socio-technical and regulatory reality. A rising number of vulnerable persons will use smart products in a domestic context for reasons such as health checks or entertainment. Due to the manner most Internet of Things (IoT) devices are currently designed, as their number increases, the number of security issues will unfortunately most probably rise as well. As a result, it is essential to evaluate how to ensure GDPR compliance and the respect of vulnerable people's rights in a smart home setting. Data protection provisions need to be implemented in a way that protects vulnerable users against potential breaches and helps them in deciding how their data is processed.

Concerning the definition of vulnerable people, this article discusses children as well as adults living with commonly recognised cognitive disabilities (this approach has the benefit of underscoring the most important GDPR compliance issues), notwithstanding the fact that there is a need of a wider discussion in relation to how the notion of vulnerable data subject should be defined. Interviewees in this study have provided their own suggestions and opinion on this topic, and their views will be discussed in more depth in subsequent sections.

2. The process and nature of this empirical study

This section introduces the methodological aspects of gathering information through semi-structured interviews conducted with UK, EU and international professionals. An interdisciplinary approach has been chosen. Both technologists and lawyers were interviewed as the disciplines they represent play a crucial role in this legal and computer science-related setting. Those discussions gave various insights and perspectives into

[3]See, for example, Stanislaw Piasecki and Jiahong Chen, 'Complying with the GDPR When Vulnerable People Use Smart Devices' (2022) 12(2) International Data Privacy Law 113 as well as Gianclaudio Malgieri and Jędrzej Niklas, 'Vulnerable Data Subjects' (2020) 37 Computer Law & Security Review 105415.

[4]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, GA Res. 44/25, annex, 44 UN GAOR Supp. (No 49) at 167, UN Doc. A/44/49 (1989).

how the two communities view intricate practical data protection challenges. 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 article. 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 work, that is the question of 'how knowledge is generated and, further, how relations of power influence the processes of knowledge generation', this article will now explain its epistemological assumptions, methods, methodology and data analysis processes.[5] In this study, 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'.[6] Interpretive research was used to analyse how technologists and lawyers subjectively perceive GDPR compliance issues when vulnerable people use smart products. More precisely, an interpretative phenomenological approach was adopted, 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.[7] The goal of this epistemological stance was to present a more critical commentary of the interviewees' activities and viewpoints.

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.[8] 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.[9] 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

[5]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.
[6]Geoff Walsham, 'Doing Interpretive Research' (2006) 15(4) European Journal of Information Systems 320, 320.
[7]Carla Willig, *Introducing Qualitative Research in Psychology* (2nd edn, McGraw-Hill Education 2008) 17.
[8]Victoria Clarke and Virginia Braun, 'Thematic Analysis' (2017) 12(3) The Journal of Positive Psychology 297, 297.
[9]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.

final "outcome" of data coding and iterative theme development'.[10] In the context of this article, 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).[11] As a result, the analysis that this article 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'.[12] Themes are, in contrast to codes 'like multi-faceted crystals – they capture multiple observations or facets'.[13] They are often developed from several codes, although rich and multifaceted codes can sometimes be elevated into the theme category.[14] Most importantly, 'themes are patterns of shared meaning, united by a central concept or idea' that can gather together data, which could at first appear quite heterogeneous.[15] 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'.[16]

The choice of semi-structured interviews (instead of fully structured ones) and the resulting 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. The interview questions were centred around what this article considers as the most relevant data protection principles in the context of this study, namely the various legal bases, the transparency principle, fairness, data minimisation, data protection by design and by default (DPbDD), data protection impact assessments (DPIAs), standards and certification schemes as well as the privacy-as-confidentiality versus privacy-as-control and edge computing versus cloud computing debates. 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 products. Questions were refined and evolved during data collection to gather richer data, in line with the reflexive thematic analysis process.[17] Answers were provided by experts in the field and, as a result, the influence of my own values and interests was limited.

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 on the practical

[10]Braun and Clarke, 'One Size Fits All? What Counts as Quality Practice in (Reflexive) Thematic Analysis?' 333 (n 9).
[11]Virginia Braun and Victoria Clarke, 'Using Thematic Analysis in Psychology' (2016) 3(2) Qualitative Research in Psychology 77, 84.
[12]Braun and Clarke, 'One Size Fits All? What Counts as Quality Practice in (Reflexive) Thematic Analysis?' 340 (n 9).
[13]ibid.
[14]ibid.
[15]ibid 341.
[16]ibid 331.
[17]Braun and Clarke, 'Conceptual and Design Thinking for Thematic Analysis' 12 (n 9).

aspects of data protection law compliance. However, several academics were interviewed as well, as they have also participated in university or industry projects related to smart devices and 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.[18] Indeed, it is not 'philosophically and methodologically consistent with reflexive TA'.[19] 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.[20] 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'.[21] 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 (both small and big companies being represented as well as lawyers and academics), it was the perceived 'information power' of this data set that resulted in the decision to end the data collection process.[22]

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 (Tables 1 and 2).

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 with various subthemes, and further regrouped during the last stage of reflexive TA (report writing) into the following sections: a vulnerability-aware approach (Section 3), legal GDPR compliance challenges for companies and professionals (Section 4) and the need of a privacy-preserving holistic technological model (Section 5). All discussions with interviewees organised within the latter responded to at least one of the two research questions of this article, 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 study strived to analyse the attitudes of experts to GDPR compliance. Not all sections

[18]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.
[19]Braun and Clarke, 'Conceptual and Design Thinking for Thematic Analysis' 15 (n 9).
[20]Braun and Clarke, 'To Saturate or not to Saturate?' 207 (n 18).
[21]Braun and Clarke, 'Conceptual and Design Thinking for Thematic Analysis' 17 (n 9).
[22]Braun and Clarke, 'To Saturate or not to Saturate?' 12 (n 18).

Table 1. Lawyers and data protection officers (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 technology development company	13 years	Law, technology, ethics and society, data protection
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

and sub-sections are of equal length as only discussions relevant to this article's topic were retained during report writing. Finally, the sixth section offers a more condensed discussion of the findings 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 6).

3. Vulnerability-aware approach

3.1. All data could be personal

The distinction between personal and non-personal data is becoming increasingly blurred. 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.[23] 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

[23]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.

Table 2. 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 small and medium-sized enterprise (SME)	17 years	Artificial intelligence, smart devices, technology development
Charlotte	Researcher at US university, Educator on the Internet of Things (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

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. This article 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. 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.

Responses from interviewees are largely in line with the opinion 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 small and medium enterprise (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:

> 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.

3.2. 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. Six 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. The layered approach was proposed in academic literature through Luna's theory of layered vulnerability (also reflecting GDPR's risk-based approach).[24] Vulnerability is certainly a very context-specific notion and a broader discussion as well as 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 data protection authorities (DPAs) so that they are actually followed by organisations developing smart products.

3.3. Education, guidance and enforcement as solutions

Education and awareness are needed in relation to data protection law, both in relation to the public and experts. This 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

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

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. 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 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 European Data Protection Board's (EDPB) plans to issue guidelines on processing of children's data that never came into fruition. Avena ((Data Protection Officer) 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. 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.[25] Seven 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).[26] However, apart from pointing this out, interviewees did not suggest any

[25]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.

[26]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/

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. 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.

3.4. An approach beneficial to all data subjects and data controllers

Interviewees stated 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 (Chief Technology Officer (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?

4. Legal GDPR compliance challenges for companies and professionals

4.1. Implementation of Article 5.1 (a) GDPR: lawfulness, transparency and fairness

4.1.1. 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 (for example, in relation to the balancing exercise when organisations use legitimate interests). These violations could be poten-

press-releases/data-protection-commissions-two-statutory-inquiries-facebooks-processing-childrens-data-instagram> accessed 2 June 2023.

tially prevented through a collaborative work of designers and regulators to create tools permitting quick discovery of GDPR infringements.[27] The empirical study underscored the need of technological practical solutions.

Concerning consent (Article 6.1 (a) GDPR), 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 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'. 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 is age identification online. As Neda (Professor of Law) stated, they 'have

[27]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).

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. 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'.[28]

Legitimate interests (Art. 6.1 (f) GDPR) have 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 are 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'.[29] 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 basis currently depends on many companies' willingness to truly satisfy its requirements, until enforcement of legal provisions becomes reality.

Concerning performance of a contract (Art. 6.1 (b) GDPR), 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

[28]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 2 June 2023.

[29]Art. 6.1 (f) of the GDPR states that 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*' (emphasis added).

for whom the services might need to be restricted or provided on the basis of another legal ground.

In terms of vital interests (Art. 6.1 (d) GDPR), 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.

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.

4.1.2. Transparency as a difficult but crucial principle

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.[30] While measures adopted for children will certainly 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.[31] 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, for example in the UK, through the publication of the Information Commissioner's Office Age Appropriate Design report.[32]

Transparency has not been explicitly linked by experts to the publication of DPIAs, DPbDD measures, certifications, codes of conduct or other mechanisms 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.

4.1.3. Fairness as a useful but vague concept

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

[30]European Data Protection Board, '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 2 June 2023.

[31]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 2 June 2023.

[32]Information Commissioner's Office, 'Age Appropriate Design' 37 (n 28).

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 is often elusive within DPIAs and it is 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 it is essential to work 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.

4.2. Data minimisation

4.2.1. Tension with device usefulness

Discussions with interviewees have shown that a tension currently exists between data minimisation (Article 5.1 (c) GDPR) 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.[33] However, there are important risks of GDPR violations linked to IoT products considering the excessive data collection practices often associated with their use.[34] 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

[33]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.
[34]Piasecki and Chen (n 3).

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 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?

4.2.1. 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 modellers 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 study considers data minimisation as a particularly relevant principle in the context of vulnerable persons using smart products.

4.2.3. Compliance approaches and solutions do data minimisation

This article 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 many interviewees (nine persons) 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 (this project will be further discussed later in this study) 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.

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 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.

4.3. Data protection by design and by default

4.3.1. Data protection is essential for vulnerable individuals and beneficial for companies

Considering the fact that DPbDD is an overarching principle, essential for the implementation of all GDPR principles, by design measures are certainly both an opportunity and a challenge to ensure greater GDPR compliance.[35] 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 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,

[35]European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (n 30).

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, data protection by design is not only about security and data minimisation. It is also essential, for example, in the context of transparency.[36] 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.

4.3.2. Experts' knowledge of DPbDD and the application of the 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.[37] For this to happen, it is essential that all terminology is correctly comprehended and defined.

Perhaps surprisingly, not many interviewees (6 out of 21) mentioned data protection by default measures whereas they are essential in the context of vulnerable adults using smart products.[38] 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

[36]Sandra Wachter, 'The GDPR and the Internet of Things: A Three-Step Transparency Model' (2018) 10(2) Law, Innovation and Technology 266.
[37]Mireille Hildebrandt and Laura Tielemans, 'Data Protection by Design and Technology Neutral Law' (2013) 29(5) Computer Law & Security Review 509.
[38]Piasecki and Chen 128 (n 3).

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 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, 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.

4.4. Data protection impact assessments as multifaceted instruments of evaluating risks

Data protection impact assessments (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. They are required by the GDPR when vulnerable people use smart devices as this represents a situation that could result in high data protection risks.[39] This article 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 data protection authority. 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 data protection authorities to work with organisations like Avena's and engage with

[39]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 2 June 2023.

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.[40] 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 align with the rights-based and values-oriented impact assessment model proposed by Alessandro Mantelero (or at least to go beyond data protection considerations).[41] 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 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

[40]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.

[41]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.

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. 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.

4.5. Uncertainties around certification and standards as compliance tools

Many organisations do not implement effective standards or ignore some of their requirements.[42] 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.[43] 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. 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.[44] Harmonised standards are considered by the Court of Justice of the European Union (CJEU) as part of EU law, which greatly increases their potential for implementation in practice.[45] 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, 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

[42]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.

[43]TSA, 'The Quality Standards Framework' (2022) <https://www.tsa-voice.org.uk/-covid-19/safe-working-environments/quality-standards-fr/> accessed 2 June 2023; ID Cyber Solutions, 'Cyber Essentials Plus' (2022) <https://cyberessentials.online/cyber-essentials-plus/> accessed 2 June 2023.

[44]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.

[45]James Elliott Construction Limited v Irish Asphalt Limited, Case C-613/14, [2016] (ECLI:EU:C:2016:821); European Commission, 'Harmonised Standards' (2019) <https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en> accessed 2 June 2023.

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 should take this into consideration during their development.[46] 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, certifications can not only increase GDPR compliance (for example, in relation to the transparency principle) but also increase customers' trust in products and companies.[47] However, the assumptions upon which they are based and the criteria against which they are evaluated need to be carefully thought-through. Ten 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.

5. The need of a privacy-preserving holistic technological model

5.1. 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 supporting them in developing tools that follow privacy by design

[46]See, for example, Department for Culture, Media and Sport, '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 2 June 2023; British Standards Institution, '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 2 June 2023.

[47]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); 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).

principles. In this regard, this article 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.[48]

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.

5.2. Security and confidentiality

5.2.1. Impossible perfection of security measures

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, 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 article arrives at is that in the context of vulnerable

[48]European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (n 30).

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.

5.2.2. 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. It has important practical implications and discussions with interviewees shined a light on how professionals perceive this contentious topic.

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.

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.[49] 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 within their homes. How confidentiality and control interact with other rights vulnerable people may have requires additional studies.

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.

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

> 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.

5.3. 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. Problems related to age assurance continue to exist and there are no adequate solutions.[50] 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. 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. 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

[50]Information Commissioner's Office, 'Age Appropriate Design' 35 (n 28).

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 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.

5.4. 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 article will provide ideas 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).[51] 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.

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

[51] 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, '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 2 June 2023, 49–50).

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.[52] Indeed, this standard has been recently launched by the Connectivity Standards Alliance (CSA) and over 280 companies.[53] 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'.[54] 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 article strived to show some of the merits and challenges of edge architectures mentioned by interviewees. They could become comprehensive data management solutions to GDPR compliance and should be critically evaluated.[55]

6. A summary of this article's findings

6.1. 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

[52]Silicon Labs, 'CHIP 180 - Connected Home over IP' (2022) <https://www.silabs.com/support/training/connected-home-over-ip-intro> accessed 2 June 2023.

[53]VentureBeart, 'How Matter 1.0 will Enable Smart Home Devices to Work Together with All Major Ecosystems' (2022) <https://venturebeat.com/ai/how-matter-1-0-will-enable-smart-home-devices-to-work-together-with-all-major-ecosystems/> accessed 2 June 2023.

[54]Connectivity Standards Alliance, 'Matter, The Foundation for Connected Things' (*CSA*, 2022) <https://csa-iot.org/all-solutions/matter/> accessed 2 June 2023; CSA, 'Building the Foundation and Future of the IoT' (*CSA*, 2022) <https://csa-iot.org/> accessed 2 June 2023.

[55]For a recent discussion on this topic see, for example, Stanislaw Piasecki, Jiahong Chen and Derek McAuley, 'Putting the Right P in PIMS: Normative Challenges for Protecting Vulnerable People's Data through Personal Information Management Systems' (2022) 13(3) European Journal of Law and Technology 1.

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.

6.2. Analysing professionals' approach to GDPR implementation when vulnerable people use smart devices

The business reality is that consent is portrayed as the least popular legal basis by most companies developing smart products used by vulnerable individuals because of the additional legal hurdles associated with this legal basis in this specific context and due to the high bar of consent requirements in general. Some also consider that consent may be negative for vulnerable people 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 persons' rights depends on whether a company has actually gone through in-depth balancing exercises.

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 this 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.[56] Fairness might need to be

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

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 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). 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, for example, Mantelero's more specific recommendation to follow a rights-based and values-oriented model).[57] Vulnerable people themselves or their carers could be included in some DPIAs, depending on their condition, the level of required technical expertise and resources of the organisation.

[57]Mantelero (n 41).

When they implement them, companies use a variety of mechanisms and standards to certify 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.

6.3. 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.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The author was supported by the Engineering and Physical Sciences Research Council [grant number EP/L015463/1].

ORCID

Stanislaw Piasecki http://orcid.org/0000-0001-5748-8631