



Complying with the GDPR when vulnerable people use smart devices

Stanislaw Piasecki * and Jiahong Chen **

Abstract

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

Background and objectives

This article critically analyses data protection compliance issues when organizations develop and deploy

smart devices used by vulnerable people. It focuses on inherently vulnerable adults and children, and analyses how to best protect their data. Complying with the General Data Protection Regulation (hereinafter 'GDPR') provisions related to the processing of vulnerable people's data would be beneficial not only for the latter but also for organizations developing and deploying smart products. Companies could avoid fines, business disruption, and gain trust of their customers by protecting their vulnerable customer's rights. Smart devices are used by vulnerable individuals, regardless of whether they are designed specifically for them or for the general population (eg, smart door locks, smart alarms, or voice assistants). The GDPR has various provisions related to vulnerability, and organizations need to comply with them. For example, it requires organizations to adopt special measures to protect children's rights (recital 38).¹ Some of those measures could be beneficial for all people (eg, writing privacy policies in a child-friendly language), while others would need to be adapted to the needs of particular groups of vulnerable individuals (eg, in the case of smart devices sold to people living with dementia). Informational privacy is essential to the recognition of children and vulnerable adults as people whose dignity is protected.² Apart from international treaties such as the United Nations Convention on the Rights of the Child, the GDPR also recognizes an inherent link between informational privacy and human dignity in its Article 88.³ What kind of measures should organizations take to comply with the GDPR when their smart products are used by vulnerable people? On which GDPR principles should they focus?

* Stanislaw Piasecki, PhD Student, Horizon Digital Economy Research, University of Nottingham, Nottingham, UK

** Jiahong Chen, Lecturer in Law, School of Law, University of Sheffield, Sheffield, UK

SP is supported by the Horizon Centre for Doctoral Training at the University of Nottingham and the Engineering and Physical Sciences Research Council (grant number EP/L015463/1). JC is supported by the Engineering and Physical Sciences Research Council (grant numbers EP/M02315X/1, EP/T022493/1, EP/R03351X/1).

- 1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation, 'GDPR') [2016] OJ 2016 L 119/1.
- 2 JC Buitelaar, 'Child's Best Interest and Informational Self-Determination: What the GDPR can Learn from Children's Rights' (2018) 8(4) International Data Privacy Law 293.
- 3 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).

This article first briefly defines smart homes and vulnerable individuals. In the following sections, it analyses the choice of a legal basis (lawfulness principle) and other relevant GDPR principles in this particular context.

A brief definition of smart homes and vulnerable people

Defining vulnerable individuals

The GDPR states that the parental consent mechanism generally applies when the child is younger than 16 years.⁴ Processing personal data will be lawful only if the child's parent or custodian has consented to such processing.⁵ However, Member States are allowed to lower this threshold in national legislation up to 13 years old. Children are the only group of vulnerable people that is explicitly mentioned in the GDPR (recital 38, recital 58, recital 65, recital 71, recital 75, Article 6.1 (f), Article 8, Article 12, Article 40.2 (g), and Article 57.1 (b)) and the only time that the term vulnerability appears is in recital 75, which states that 'the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage,' especially 'where personal data of vulnerable natural persons, in particular of children, are processed'. The GDPR therefore places emphasis on children as requiring particular attention while not excluding other categories of vulnerable people, although not mentioning any explicitly. Recital 38 of the GDPR states that children's personal data require special protection measures to be taken by the data controller as they 'may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'.⁶ This should also be true for other groups of vulnerable people for whom such specific measures should be taken as well. This approach is in conformity with other European Union (EU) data protection legislation, such as Directive 2016/680, which states in recital 39 that any information provided to the

data subject 'should be adapted to the needs of vulnerable persons such as children'.⁷

As to the definition of vulnerability, the UK's Information Commissioner's Office (ICO) informs that 'individuals can be vulnerable where circumstances may restrict their ability to freely consent or to object to the processing of their personal data, or to understand its implications'.⁸ This is a very broad definition of vulnerability, encompassing a wide array of situations. This shows that ICO's objective is to cover all kinds of vulnerabilities when it comes to data protection. Concerning vulnerable adults, the ICO gives examples of older people or those living with particular disabilities while not giving a definitive list. It states that even in the case where someone cannot be automatically categorized as vulnerable, a power imbalance in their relationship with another person can create a situation of vulnerability in the context of the GDPR. An example of this are employees who can be treated as vulnerable when there is a power imbalance as a result of which they have difficulties to object to the processing of their personal data by their employer.⁹ The ICO adds that this kind of vulnerability can also arise in other circumstances, for example, in relation to an individual's financial situation (when establishing a credit rating, etc) or when a patient's data are being processed for medical care reasons.¹⁰

On the EU level, the Article 29 Data Protection Working Party (WP29) states that vulnerable data subjects can include employees, children (because they can be considered as not having the capacity to consciously and thoughtfully consent or oppose data processing activities), vulnerable groups of the population needing special protection (people with mental health problems, the elderly, patients, etc), and in any situation in which an imbalance of power between the controller and the data subject exists.¹¹ This is a large definition and non-exhaustive list of vulnerable individuals, similar to ICO's guidelines.

Vulnerability conveys a large diversity of fact-based situations. The wide range of mental and physical

4 GDPR, art 8.

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

6 *Ibid.*

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

8 Information Commissioner's Office, 'When Do We Need to Do a DPIA?' <<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 6 October 2021.

9 Art 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (WP 248, 4 October 2017).

10 ICO, 'When Do We Need to Do a DPIA?' (n 8).

11 Art 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA)' (n 9).

conditions that are relevant requires a flexible approach. Anyone can become vulnerable under particular circumstances. Legislation and relevant actors should be responsive and adaptive when this happens. The approach of the European Court of Human Rights (ECtHR) reflects this as it builds an ever-expanding case law on existing and emerging groups of vulnerable people. This can help in the mission to achieve a more ‘robust idea of equality’.¹²

While vulnerability has been rarely explored by privacy and data protection researchers, Malgieri and Niklas recently analysed ‘the role and potentiality of the notion of vulnerable data subjects’.¹³ They stated that vulnerability can be viewed as universal (all individuals are equally vulnerable) or particular (some individuals are more vulnerable than others). Indeed, researchers have previously argued in favour of both. According to Fineman, vulnerability is a universal element of the human condition and shared by all while Cooper underlines that while this may be true, a universal approach conceals the specific experiences based on identities, such as those of young men of colour who ‘continue to be always already suspect to the police’.¹⁴ Malgieri and Niklas consider that ‘situating vulnerability in the data protection framework is a problematic task’ because if all data subjects are considered universally vulnerable, then important differences between them could be ignored (thereby exacerbating the already disadvantageous position of some persons), while making data protection rules and safeguards more specific could result, among other issues, in the fragmentation of an already complex legal landscape.¹⁵ As a solution to this conundrum, they propose Luna’s theory of layered vulnerability.¹⁶ Luna overcomes the universal versus particular divide by arguing that all people are vulnerable but that some persons possess more vulnerability layers than others. This layered approach seems to reflect GDPR’s risk-based approach, the latter suggesting that anyone can be vulnerable but at various levels and in different contexts. It also reflects Calo’s stance that ‘no one is entirely invulnerable at all times and in all

contexts’ and that ‘we are all vulnerable in degrees and according to circumstance’.¹⁷ Calo argues that while the law usually considers vulnerability as a status of a person or group or as a relationship between individuals and organizations, legal research increasingly acknowledges that this concept is best perceived as ‘layer of personhood’, a condition that exists more frequently and intensively in some individuals and contexts, but in all people sometimes.¹⁸ How does this debate translate into the contribution that this article is trying to make in the data protection field?

This study agrees that layers of vulnerability can manifest in any person and that the layered approach has the benefit of taking everyone into consideration, even the most subtle cases of vulnerability, while also promoting an intersectional and cumulative approach. However, it also argues that in some situations, categorizing vulnerable individuals can be helpful to ensure a higher level of their data protection. This article does not focus on ‘contextual’ vulnerability but rather on children and adults who are considered inherently vulnerable, that is whose layers of vulnerability are constantly and unequivocally present, such as adults with disabilities. Children ‘have limited capacity to understand the complexity of data-driven architecture, have less experience, less awareness of risks and rights and may be easily manipulated’ (this is reflected in GDPR’s provisions), while the inherent vulnerability of adults with disabilities has been confirmed in the case law of the ECtHR.¹⁹ There are many vulnerability layers or other situations in which people could be considered as vulnerable (eg, the above-mentioned situations of imbalance of power between employers and employees) but deciding whether they actually are would require a case-by-case analysis. Those subtle vulnerabilities do not fall into the scope of this work. Such a choice of focus has the benefit of highlighting the most pressing practical challenges with less distractions from borderline cases. Of course, this does not mean that the latter are less important in any way, but that the objective of this study is to reflect more broadly on vulnerability in the GDPR and smart home context, by using examples

12 Oddný Mjöll Arnardóttir, ‘Vulnerability under Article 14 of the European Convention on Human Rights’ (2017) 1(3) *Oslo Law Review* 150; Lourdes Peroni and Alexandra Timmer, ‘Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law’ (2013) 11(4) *International Journal of Constitutional Law* 1056.
13 Gianclaudio Malgieri and Jędrzej Niklas, ‘Vulnerable Data Subjects’ (2020) 37 *Computer Law & Security Review* 105415.
14 Martha Albertson Fineman, ‘The Vulnerable Subject: Anchoring Equality in the Human Condition’ (2008) 20(1) *Yale Journal of Law and Feminism* 1; Frank Rudy Cooper, ‘Always Already Suspect: Revising Vulnerability Theory’ (2015) 93(5) *North Carolina Law Review* 1379.
15 Malgieri and Niklas (n 13) 5.

16 Florencia Luna, ‘Elucidating the Concept of Vulnerability: Layers Not Labels’ (2009) 2(1) *International Journal of Feminist Approaches to Bioethics* 121.

17 Ryan Calo, ‘Privacy, Vulnerability, and Affordance’ (2017) 66(2) *DePaul Law Review* 593.

18 *Ibid.*

19 Alexandra Timmer, ‘Vulnerability: Reflections on a New Ethical Foundation for Law and Politics’ in Martha Albertson Fineman and Anna Grear (eds), *A Quiet Revolution: Vulnerability in the European Court of Human Rights* (Ashgate, Farnham 2013); Alexandra Timmer, ‘Strengthening the Equality Analysis of the European Court of Human Rights: The Potential of the Concepts of Stereotyping and Vulnerability’ (Doctor of Law, Universiteit Gent 2014); Malgieri and Niklas (n 13).

data, storage in cloud databases, and various data privacy threats associated with it.²⁷ The scale of recent data breaches shows that this is likely to happen.²⁸

Consumers are rarely conscious of the risks to their data when they use smart products and do not possess technical capacities to set up a safe smart home environment.²⁹ They frequently have problems with device management as well as network management. As a consequence, smart devices should be given special attention by policy makers as well as those developing and deploying them. People will be able to effectively manage their devices and networks (and therefore protect their data) only if this is made easy for them.³⁰

Threats linked to IoT home products are not a recent problem and some are well known for a long time now. Already in 2014, the WP29 had recognized the existence of various threats to personal data security arising from smart devices.³¹ Those threats are linked to consumers being monitored by third parties and not having real control over how their personal data are exploited. Other risks are related to modifying the purpose of processing people's data, profiling techniques, and gaining information about users' behaviour patterns. Staying anonymous has become increasingly difficult for people who own IoT devices within their homes.³² People can also be victims of identity theft, cyber harassment, and discrimination, and have their reputation tarnished because of leaks and takeovers of data. Moreover, cybercriminals do not stop inventing new threats and they are often successful in overcoming security barriers. Vulnerable people may have lower capacities to defend themselves against such data security risks. The GDPR recognizes that there is a need to adapt data protection mechanisms to vulnerable people's needs (eg, recital 38 and recital 75 of the GDPR).

New technologies have been used to help vulnerable individuals in various ways for a long time now. People with different health conditions or simply experiencing symptoms associated with old age have been able to live more autonomously as a result of technological

advances. This has been the subject of a longstanding line of research in computing under the heading of ambient assisted living. The use of smart devices is just the latest development in this field. Exploring how those products process vulnerable people's data is crucial. Vulnerability can have consequences either during data processing (eg, there may be more risks for some persons in terms of providing informed consent) or as a result of the processing (data processing could lead to discrimination or, eg, psychological harms).³³ Among smart devices, some of them are targeting specific categories of individuals.³⁴ In the case of children, new Internet-connected toys have been appearing on the shelves of shops such as interactive dolls or robots.³⁵ Parents also purchase products such as smart baby monitors or smart watches that track their child's sleep patterns, location, and medical data.³⁶ In the case of people living with dementia, there are many health devices or tracking devices developed to support them in their daily activities.³⁷ IoT products targeting specific parts of the population require a more focussed approach from data controllers based on the consumers' specific layers of vulnerability [and on data protection impact assessments (DPIAs) that organizations should conduct in this context] as this could help in ensuring that measures are better adapted to their needs at the data processing stage. Widely used devices, such as voice assistants, are more difficult to adapt to everyone as everyone's layers of vulnerability are different. This could be partly tackled by preventing potential negative effects of data processing through more general data protection safeguards [implementing the data protection by design and by default (DPbDD) principle], which will be explored later in this article.

As a consequence of the rapid expansion of the IoT world and the fact that an increasing number of people will live within smart homes over time, it is crucial to discuss how to best protect personal data of those who are the most vulnerable. Because of the way most IoT devices are currently designed, as their number

27 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.

28 Gartner, 'Leading the IoT: Gartner Insights on How to Lead in a Connected World' (2017) 13 <https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf> accessed 6 October 2021.

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

30 Anne Adams and Martina Angela Sasse, 'Users are Not the Enemy' (1999) 42(12) *Communications of the ACM* 40.

31 Art 29 Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (WP 223, 16 September 2004).

32 Ibid.

33 Malgieri and Niklas (n 13).

34 Brent Arnold and Kavi Sivasothy, 'He Sees You when You're Sleeping, He Knows When You're Awake: Smart Toys and Regulating the IoT in Canada' (*Gowling WLG*, 17 December 2018) <<https://gowlingwlg.com/en/insights-resources/articles/2018-smart-toys-and-regulating-the-iot-in-canada/>> accessed 6 October 2021.

35 Lisa Collingwood, 'Villain or Guardian? "The Smart Toy is Watching You Now . . ."' (2021) 30(1) *Information & Communications Technology Law* 75.

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

37 Grant Gibson, 'Smart Technologies in Dementia Care – Future Opportunities and Challenges' (21 March 2019) <<https://dementia.stir.ac.uk/blogs/dementia-centred/2019-03-21/smart-technologies-dementia-care-future-opportunities-and/>> accessed 6 October 2021.

protection authority has suggested, for example, to present privacy notices in clear, plain, and age-appropriate language.⁴⁴ What this article considers is that for smart devices used by everyone (eg, voice assistants), measures supporting vulnerable individuals (such as those proposed by the UK's ICO in its Age Appropriate Design code of practice) should be automatically adopted for all data subjects. First, this would facilitate data protection compliance with provisions related to vulnerable people mentioned above. Secondly, using simple terms and clear concepts should be a standardized practice for all privacy policies as most people cannot comprehend the technical and convoluted language that they usually adopt.

In terms of sensitive data, there is a corresponding legal basis to ordinary consent called explicit consent. A two-step verification process (eg, asking the data subject to send an email containing the statement 'I agree' for the data to be processed and to also click a verification link to confirm their choice) or obtaining a digital signature from the data subject (in addition to all of the previously mentioned ordinary consent conditions) seems necessary if the organization in question decides to process sensitive data through its smart devices.⁴⁵ In the current state of the IoT sector, many products used by vulnerable individuals (voice assistants, smart TVs, smart health devices, etc) do (or might) collect sensitive data and those additional explicit consent requirements would most probably apply in many situations. For example, Amazon was sued in 2019 for allegedly recording children without their or their legal guardians' consent. The complaint stated that 'at no point does Amazon warn unregistered users it is creating persistent voice recordings of their Alexa interactions, let alone obtain their consent to do so.'⁴⁶ At the time of these events, Alexa's privacy notice only informed that previous voice requests are analysed to improve its functioning but did not explicitly state that humans listen to them. Such

voice recordings can contain sensitive data of vulnerable individuals and if the complaint had been raised in an EU context, Amazon's activities would be most probably considered as violating GDPR's provisions. In this case, Amazon should have ensured a two-step consent verification process is in place, adapted to the needs of children using its devices. Strong enforcement mechanisms are required to ensure the consent requirements are met.

Consent is not universally accepted as a useful mechanism and it has been criticized by various authors, in particular in the context of vulnerable people's data collection. Some researchers contend that consent provides an illusion of control⁴⁷ and that it is often given in the context of an imbalance of power so not accorded freely.⁴⁸ Several articles underline the nature of networked environments that establish power imbalances and reduce people's influence and control over their own personal data.⁴⁹ Vulnerable people such as children cannot fully control their personal data online because their decisions and data management options depend on the functionalities and design of communication spaces.⁵⁰ This is true for smart devices as well. Communication spaces are designed by organizations, so usually, unless the organization is a charity or similar actor (or there is a financial incentive), it will design it in a way to promote its own business interests. Smart devices asking for consent often use hardly understandable privacy policies and users do not actually familiarize themselves with them. Privacy policies for children are especially confusing, difficult to comprehend, often long and complex.⁵¹ Organizations developing smart devices could be hopefully forced to change their behaviour if enforcement, and the resulting effective implementation of GDPR, gains momentum. For this to happen, more funding should be dedicated to currently underfunded data protection authorities.⁵² An interesting idea is for designers to support regulators (and not

Children' (2018) 23(1) Communications Law 7.) These are all open questions that society needs to find a response to. A legal guardian should not have unlimited access to a vulnerable person's data as they might not always have good intentions or the capacity to make informed decisions on behalf of the person they are supposed to protect. Law provisions are unlikely to be a successful solution on their own and should be combined with technological developments in the field of data protection management to make them effective (such as personal information management systems and other privacy enhancing technologies). This topic requires further academic work.

44 ICO, 'Age Appropriate Design' (n 20).

45 EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (4 May 2020) 21 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 6 October 2021.

46 Leo Kelion, 'Amazon Sued over Alexa Child Recordings in US' *BBC* (2019) <<https://www.bbc.com/news/technology-48623914>> accessed 6 October 2021.

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

48 Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US footsteps?' (2017) 26(2) *Information & Communications Technology Law* 146.

49 Mireille Hildebrandt, 'Profiling and the Rule of Law' (2008) 1(1) *Identity in the Information Society* 55; Macenaite and Kosta (n 48).

50 Alice Marwick and Danah Boyd, 'Networked Privacy: How Teenagers Negotiate Context in Social Media' (2014) 16(7) *New Media & Society* 1051; Macenaite and Kosta (n 48).

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

52 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.

just data subjects or platforms) by designing automated tools allowing for quick discovery of GDPR violations and enforcement.⁵³ This idea was presented in the context of dark patterns associated with most current consent management platforms. Such automated tools could potentially also be designed for IoT products.

As mentioned above, even if privacy notices are written in clear terms, it is widely known that people rarely read them. This is why consent should be combined with other mechanisms providing relevant information to users (of course also in a clear and plain manner) after they have consented such as contextual pop-ups explaining how data are processed by an IoT product and allowing the data subject to easily change the settings.

Evaluating the perspective of an average data subject before processing vulnerable people's data based on a contract

The performance of a contract legal basis is lawful when processing personal data is 'necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract' (Article 6.1 (b) GDPR). The data subject must reasonably expect the use of this legal basis by the data controller. The controller should carefully evaluate the 'perspective of an average data subject' to ensure that the purpose of data processing is mutually genuinely understood.⁵⁴

In an investigation concerning visual and audio personal data processing through Philips smart TVs by TP Vision, the Dutch Data Protection Authority declared that 'a justification for the processing must be present in relation to the specific, individual data subject involved.'⁵⁵ Buying a smart TV is essentially a sales contract that has not much to do with audio or visual data. However, smart TVs often collect the latter. The performance of a contract legal basis is not the right legal basis to process personal data in this context. If a person is vulnerable, this would make the use of this legal basis even less appropriate. It is not possible to expect an ordinary person and even less a child or a vulnerable adult

to know that by turning on a TV and clicking 'I agree' at the end of long terms and conditions, they sign a contract for their vocal and visual personal data to be processed. The data controller needs to evaluate the perspective of the user to ensure that they genuinely understand the purpose of data processing.

In the case of adults with disabilities and children, there are smart products collecting health data (which falls into the sensitive category) that could be necessary, for example, for the purposes of a medical diagnosis or the provision of health care. In this situation, Article 9.2 (h) could apply and provide for a special category legal basis that is related to and could be used in combination with performance of a contract. Indeed, a contract with a health professional could allow to lawfully process sensitive data of a vulnerable person gathered through a smart home product.⁵⁶

Balancing the legitimate interests of a data controller against those of vulnerable people

Legitimate interests have become often used as a legal basis to process personal data, especially in the commercial and new technologies field.⁵⁷ For example, in relation to its Nest smart home devices, Google states that it may process individuals' information 'to pursue legitimate interests such as providing, maintaining and improving our services to meet the needs of our users.'⁵⁸ According to Article 6.1 (f) of the GDPR, processing personal data is lawful when it is:

necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The use of the term 'in particular' suggests that the balancing exercise concerning processing of children's personal data will be stricter.⁵⁹ If a compelling interest can be identified, risks to children's rights would need to be mitigated as much as possible.⁶⁰ Adults with disabilities should also benefit from appropriate protection measures if the legitimate interest legal basis is used by a data

53 Nouwens (n 40).

54 Ibid.

55 European Audiovisual Observatory, 'Smart TV and Data Protection' (2018) 60 <<https://rm.coe.int/iris-special-2015-smart-tv-and-data-protection/1680945617>> accessed 6 October 2021.

56 GDPR, art 9.2(h).

57 Federico Ferretti, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?' (2014) 51(3) Common Market Law Review 843.

58 Google, 'Technologies' (2021) <<https://policies.google.com/technologies/partner-sites?hl=en-US>> accessed 6 October 2021.

59 Ingrida Milkaite and others, 'The General Data Protection Regulation and Children's Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society. Roundtable Report' (2017) 12 <https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf> accessed 6 October 2021.

60 Centre for Information Policy Leadership, 'GDPR Implementation in Respect of Children's Data and Consent' (2018) 6 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf> accessed 6 October 2021.

controller. The WP29 confirms this by underlining that during the legitimate interests balancing test, the status of the data subject is important and that it is relevant to consider whether the data subject is a vulnerable person requiring special protection ‘such as, for example, the mentally ill, a student, a patient, or whether there is otherwise an imbalance in the relationship’.⁶¹ Legitimate interests can only be an appropriate legal basis when an organization plans to use someone’s personal data in ways that this person would reasonably expect and that have only a minimal impact on privacy, or in the case where there is a convincing reason for the processing.⁶²

One of the objectives of a smart TV seller is to provide a platform for advertisements and the associated analysis of viewer behaviour.⁶³ However, this kind of data processing is not essential to the provision of the main service. The ICO calls this ‘non-core’ processing.⁶⁴ In this scenario, it is unlikely that a child would reasonably expect that their data will be processed for advertising reasons. Moreover, no compelling interest seems to exist here that would override the need to protect fundamental rights and freedoms of vulnerable individuals. In this context, the service provider should probably rely on consent instead of legitimate interests and give the data subjects the choice to switch on different additional elements of the service whenever this is technically possible (instead of turning them on by default).

According to one opinion, the use of the legitimate interests legal basis by a data controller will often necessitate deeper reasoning, strategizing, and attention for lawful implementation in comparison to only asking for consent.⁶⁵ Considering that the legitimate interests legal basis entails a balancing of interests and risk assessment, paired with the necessity to adopt suitable mitigating measures and accountability from data controllers, it could be a solid framework for analysing risk on an individual basis and permitting for particular risks to be addressed in specific situations (in keeping with this logic, it would help in adapting measures to the interests of children and adults with disabilities).⁶⁶ As a consequence, legitimate interests should be viewed positively and recommended as a lawful legal ground to process

personal data in relevant circumstances. It should however be noted that there is no corresponding exemption under Article 9 and hence legitimate interests would not be an appropriate legal ground if sensitive data are involved.

The above-mentioned opinion assumes that organizations actually take time and effort to do the in-depth balancing tests. In the past, there have been reports that legitimate interests are seldom reviewed in practice.⁶⁷ Other authors point out that the balancing exercise is difficult and that it should not be performed only by data controllers.⁶⁸ The test necessitates a significant level of legal expertise and puts data controllers in a situation of ‘clear conflict of interest’.⁶⁹ There is an intrinsic imbalance of powers between the controller who determines whether a legitimate interest exists and the data subject who needs to accept the decision of the controller. Companies should be prevented from processing vulnerable people’s data based on unbalanced ‘legitimate interests’, for example, if they establish profiles of children, which is in general prohibited.

Considering the increasing ubiquity of smart devices, children and adults with disabilities will be using them more frequently. While smaller organizations might struggle with balancing exercises because of the lack of legal expertise or funds to hire a lawyer, big companies do not have any excuses not to perform a balancing test and should be held accountable if they do not, especially when their products are used by vulnerable people who require additional protection measures.

The rarely used vital interests legal basis

Article 6.1 (d) of the GDPR states that an organization can process personal data when this is ‘necessary in order to protect the vital interests of the data subject or of another natural person’. In the majority of cases, a situation in which vital interests will need to be protected will most probably arise in relation to health data. Health data are one of the special categories of data and, therefore, require to satisfy a condition for processing under Article 9 of the GDPR in addition to the condition from Article 6.⁷⁰ One of the special

61 Art 29 Working Party, ‘Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC’ (WP 217, 9 April 2014).

62 Information Commissioner’s Office, ‘Legitimate Interests’ <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>> accessed 6 October 2021.

63 European Audiovisual Observatory, ‘Smart TV and Data Protection’ (n 55).

64 ICO, ‘Age Appropriate Design’ (n 20).

65 Centre for Information Policy Leadership (n 60).

66 Ibid.

67 Bits of Freedom, ‘A Loophole in Data Processing’ (2012) <https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf> accessed 6 October 2021.

68 Ferretti (n 57).

69 Ibid.

70 Ibid; Information Commissioner’s Office, ‘Vital Interests’ (2019) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/>> accessed 6 October 2021.

conditions for processing health data is to protect a person's vital interests.⁷¹ However, the data subject must be incapable of giving consent for this condition to apply. For this reason, explicit consent will be the more relevant legal basis in many situations.⁷² Are there situations in which the vital interests legal basis could apply in the context of the use of smart devices by vulnerable adults or children? Researchers from the Netherlands have created a high-tech smart bracelet, the 'Nightwatch', capable of detecting 85 per cent of night-time epileptic seizures and 96 per cent of the most severe ones.⁷³ The researchers tested the device with 28 intellectually disabled participants. The Nightwatch has the ability to inform caregivers about severe seizures happening during the night. This could be a vital product for those affected by epilepsy as sudden unexpected death is the major cause of death for those living with the condition, and for adults with a mental disability the risk of dying is even higher.⁷⁴ If the vulnerable data subject is not capable of giving consent but wears the Nightwatch smart bracelet, processing his personal data to find him on time and help him during a serious epileptic seizure must satisfy the necessity to protect vital interests condition. In such rare circumstances, this legal ground will apply.

The implementation of GDPR principles when vulnerable people use smart devices

The lawfulness principle requires the processing to take place on the basis of a legitimate ground and the various legal bases have already been analysed above. This article will now briefly discuss other principles that it considers as the most relevant in the context of this study, namely transparency, fairness, data minimization, data protection by design and default, and integrity and confidentiality. DPIAs will also be examined as they contribute to the implementation of all GDPR principles.

71 GDPR, art 9(2)(c).

72 Information Commissioner's Office, 'Vital Interests' (n 70).

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

74 Eindhoven University of Technology, 'New Epilepsy Warning Device Could Save Thousands of Lives' (2018) <<https://www.tue.nl/en/news/news-overview/24-10-2018-new-epilepsy-warning-device-could-save-thousands-of-lives/#top>> accessed 6 October 2021.

75 Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press, Cambridge 2016).

The principle of transparency and the right to be informed

The right to transparent information and communication is needed to avoid the 'blackbox society', in which our data are recorded on devices and the workings of this system remain mysterious to users.⁷⁵ If data are collected without transparent information and communication about that process, vulnerable individuals will not be able to effectively exercise their data protection rights. The principle of transparency is enshrined in Article 5.1 (a) of the GDPR which states that personal data have to be 'processed lawfully, fairly and in a transparent manner in relation to the data subject.'⁷⁶

GDPR recitals and articles are informative as to the meaning and effect of the principle of transparency. According to Article 12, information must be concise, transparent, easily accessible and intelligible, and the language must be clear and plain, especially when information is provided to children.⁷⁷ Recital 58 of the GDPR adds that 'given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.' The comprehensibility requirement has been recently explicitly extended to the more general scope of 'vulnerable groups'.⁷⁸ This article will not go into detail by analysing each transparency condition. However, a few issues will now be discussed to show that special transparency measures are needed (and required) for vulnerable individuals in the specific context of smart products.

The 'easily accessible' requirement means that the data subject should not have to search for information and that it should be instantly evident where this information can be found. Smart devices have their own particular issues that need to be overcome such as the recurring lack of a user interface.⁷⁹ Leaving the user alone to look on a website or app where the privacy notice can be found and privacy settings changed could prevent vulnerable individuals, such as elderly people, from being able to choose how their personal data are processed.⁸⁰ Delivering a hard copy instruction manual

76 GDPR, art 12(1).

77 Ibid; art 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (WP 260, 11 April 2018).

78 EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (13 November 2019) 14 <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf> accessed 6 October 2021.

79 InfoWorld, 'IoT Silliness: "Headless" Devices without a UI' (2015) <<https://www.infoworld.com/article/2867356/beware-this-iot-fallacy-the-headless-device.html>> accessed 6 October 2021.

80 Ibid.

and a URL of a webpage address at which the privacy statement and settings can be consulted is an example of one solution. Providing information orally through audio capabilities of the screenless smart devices could also be an important tool if they have such capabilities,⁸¹ especially when oral information is delivered to visually impaired persons or vulnerable people who may have problems in understanding or getting access to written information.

In terms of the clear and plain language requirement, the Court of Justice of the European Union, the European Data Protection Board (EDPB), and various authors argue that its violation is a major issue as it makes exercising data subject rights difficult.⁸² This is especially important in today's data-driven IoT world where users' profiling is widespread.⁸³ On the other hand, others underline the complexity of explaining data processing activities in clear and plain language and that this can often result in simple explanations not sufficiently reflecting the actual reality of what is happening to personal data.⁸⁴ Some researchers consider that simplifying communications can limit information's quality.⁸⁵ However, for others, 'the fact that the information is addressed to a child does not mean that the scope of such notice is reduced.'⁸⁶ This article considers that companies could provide a link to the more complicated privacy policy if users desire to read it while focusing the data subject's attention on the simplified version. Easy-to-understand notices instead of complicated privacy policies 'for adults' would be much more useful for everyone. Many non-vulnerable adults complain that privacy policies are complicated and not understandable. They would benefit from more clarity themselves.

In any case, transparency alone is not enough to protect vulnerable users' data. While it is an important element of educating users and supporting them in making informed choices, it is not possible to expect

that as long as a data subject is informed, 'they will therefore make rational choices and be able to exercise their rights.'⁸⁷ Transparency should work in conjunction with other data protection principles such as fairness and data minimization.

Fair processing of vulnerable people's data by smart devices

The fairness principle is logically very important as it should ensure that vulnerable persons benefit in the same way from GDPR protections and rights as other citizens. Just like transparency, this principle is enshrined in Article 5.1 (a) of the GDPR. To some authors 'fairness is a subjective, context-dependent and highly politicized concept' and 'a global consensus on what is fair is unlikely to emerge, in the context of algorithmic decision making or otherwise'.⁸⁸ To others, 'fairness is a broad criterion which is difficult to explicate exhaustively; it is also context dependent.'⁸⁹ While all this may be true, it is important to reflect on how fairness should be applied by data controllers in the context of this study. Organizations need to be guided as subjective interpretations will not help neither with GDPR compliance nor with protecting vulnerable people's rights. The importance of the principle of fairness in the GDPR is evidence of the increasing imbalance of power between the data controller and the data subject.⁹⁰ This imbalance of power increases even more when children or vulnerable adults use technology.

First, there is a clear link between fairness and transparency. Despite the fact that fairness is not defined in the GDPR, scholars, the WP29, and the EDPB have made some attempts to do so. They consider that this principle is related to awareness.⁹¹ The fairness principle demands that personal data should only be collected when the data subject is made aware of this processing activity.⁹² In its Age Appropriate Design report, the

81 Art 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 77).

82 *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others*, Case C-201/14, [2015] (ECLI:EU:C:2015:638); EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (n 45); art 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 77).

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

84 Bart Custers and others, 'A Comparison of Data Protection Legislation and Policies Across the EU' (2018) 34(2) *Computer Law & Security Review* 234.

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

86 Dana Volosevici, 'Child Protection under GDPR' (2019) 6(2) *A Journal of Social and Legal Studies* 17.

87 Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (2016), ssrn: 2784123 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123> accessed 8 November 2021.

88 Serge Abiteboul and Julia Stoyanovich, 'Transparency, Fairness, Data Protection, Neutrality' (2019) 11(3) *Journal of Data and Information Quality* 1.

89 Buitelaar (n 2).

90 Michael Butterworth, 'The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework' (2018) 34(2) *Computer Law & Security Review* 257.

91 Wachter (n 85).

92 *Ibid.*

ICO states that if an organization is not 'clear, open and honest' about the service it provides and how it functions, then its 'original collection and ongoing use of the child's personal data is unlikely to be fair'.⁹³ Processing is unfair if, for example, a health-related smart product monitors heartbeat data but also gathers blood oxygen levels without appropriately informing the data subject about this through the device's interface or other means.⁹⁴ While they are linked, fairness and transparency do not have the same meaning. Fairness is a tool through which transparency should be interpreted (although there are few guidelines on how to do this). If a smart device provides information transparently to the general population but not to the minority of people with mental disabilities that also use this product, this should not be considered as 'fair transparency'. More broadly, this article argues that fair transparency should be viewed as requiring organizations to adopt special data protection measures for vulnerable people by default in any smart product (such as high privacy settings, opt-in mechanisms, or child-friendly language to name a few).

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

Secondly, fairness has a crucial implicit objective to prevent mishandling of data subjects' data by data controllers through balancing exercises (an important element of how the GDPR works in practice). A balancing exercise is often implicitly required by the GDPR to be carried out by controllers.⁹⁵ Fair balancing is to be defined and evaluated on a case-by-case basis. In the context of the topic of this article, relevant guidelines are

scarce. Some can be found in the ICO's Age Appropriate Design report.⁹⁶ If vulnerable people's data are processed by a smart product, data controllers will need to take into consideration an increased power imbalance between themselves and the data subject to ensure that data processing is fair. For example, a smart device sharing children's personal data with a third party would need to be justified by a 'compelling reason to do so, taking account of the best interests of the child' in order for data processing to be fair.⁹⁷ Fair processing is context dependent and more examples of fair balancing in the IoT sector would be certainly helpful for data controllers.

Because clarifications are still needed regarding the meaning of the fairness principle, there is an opportunity to define it more holistically and to go beyond strict legal limitations in order to express data ethics initiatives.⁹⁸ According to the EU's Agency for Fundamental Rights, the concept of fairness within the GDPR can be considered as requiring data to be processed in an ethical manner and goes beyond the need to provide information transparently to the data subject.⁹⁹ The European Data Protection Supervisor has called for an urgent reflection on ethics and data protection, partly by underlining the importance of discussing how the fairness principle should be perceived in this context.¹⁰⁰

Minimizing the exposure of vulnerable people to data protection threats

As a consequence of their general vulnerability, and in conformity with the lawfulness and fairness principles, organizations targeting children with their smart products 'should even more strictly respect the principles of data minimisation and purpose limitation'.¹⁰¹ Article 5.1 (c) of the GDPR states that processing of personal data should be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.¹⁰² ENISA observed that data minimization does not only mean reducing data fields in a form but also refers to any other means of minimizing data collection and data processing activities

93 ICO, 'Age Appropriate Design' (n 20).

94 Art 29 Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 31).

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

96 ICO, 'Age Appropriate Design' (n 20).

97 Ibid.

98 Clifford and Ausloos (n 95).

99 FRA, 'Handbook on European Data Protection Law' (2018) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf> accessed 6 October 2021.

100 EDPS, 'Opinion 4/2015 Towards a New Digital Ethics' (2015) <https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf> accessed 6 October 2021.

101 Art 29 Working Party, 'Opinion 02/2013 on Apps on Smart Devices' (WP 202, 2013).

102 Ibid.

‘following not only a quantitative but also a qualitative approach’.¹⁰³ This principle is in stark contrast to the ‘data maximalism’ associated with the huge amounts of information collected by IoT products, stored and usually analysed in the cloud.¹⁰⁴ In 2013, the WP29 drew attention to the ‘alarming disregard’ of the principle of data minimization in view of the excessive data collection by many apps on smartphones, without any real relationship to the functionality of those apps.¹⁰⁵ As a result of the GDPR, data controllers now need to be ready to prove that they comply with relevant data minimization best practices and requirements in line with the overarching accountability principle.¹⁰⁶

In the specific context of smart products used by vulnerable people, one problem that comes to mind is when organizations providing information society services (ISS) record and gather personal data to identify the data subject’s age in order to know whether they need to obtain consent from a legally authorized representative before they process their personal.¹⁰⁷ Data controllers need to remember that they must comply with the principle of data minimization in this context too.¹⁰⁸ To do so, they will have to gather only the amount of personal data that are strictly necessary to inform them about the age of particular users. These data must only be used for the purpose of providing age appropriate settings and measures and not for any other purpose such as advertising (unless consent has been obtained to do so or another legal basis permits this). The Centre for Information Policy Leadership considered three ways through which a data controller could verify the customer’s age. It concluded that universal age assessment would be too intrusive while verifying the age of data subjects only when services explicitly state that they target children would be under-inclusive. As a consequence, the Centre argued in favour of performing a risk analysis by evaluating ‘whether the offering is intentionally made to be attractive to children; whether children have been attracted to the ISS or similar services in the past; and whether the registration process to the ISS reflects an assumption that the users are above the age of digital consent.’¹⁰⁹ From a data protection perspective, this article does not consider this approach as appropriate for two reasons. First, children

might be attracted to services that are not designed to be used by them and this would be difficult to verify. Secondly, it seems unrealistic to expect organizations to carry out another risk analysis, especially for smaller organizations, who already struggle with GDPR compliance. As a result, this study argues in favour of minimizing data collection through age verification mechanisms that use the best privacy preserving technologies available, to promote the use of such technologies and develop guides on how to implement them.

Of course, age verification is not the only issue that needs to be reflected upon in the context of data minimization when vulnerable people use smart products. Another one could be, for example, the need to identify the legally authorized representative to give consent on behalf of a child or on behalf of a vulnerable adult. State-of-the-art technologies could help here as well. How they can interact with legal rules to facilitate data protection compliance is not within the scope of this article but this could be the subject of future interdisciplinary studies.

Thinking about vulnerable people’s data protection throughout the development and deployment process of smart products

Article 25 of the GDPR introduces a qualified responsibility on data controllers to use technical and organizational measures, which are designed to make certain that personal data processing is compliant with GDPR’s provisions and to ensure that consumers’ data protection rights are safeguarded. This duty also concerns the default implementation of data protection principles and default boundaries on who has access to personal data.¹¹⁰ How does DPbDD apply in the context of vulnerable individuals using smart devices?

The current focus on the PET confidentiality paradigm when designing IoT products

In response to difficulties in enforcing legal provisions by underfunded data protection authorities, a set of technical approaches emerged under the name of privacy enhancing technologies (PETs) to allow for more responsible and effective processing of personal data, often in the context of implementing privacy by design.¹¹¹

103 ENISA, ‘Recommendations on Shaping Technology According to GDPR Provisions - Exploring the Notion of Data Protection by Default’ (2018) <<https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2>> accessed 6 October 2021.

104 Wachter (n 85).

105 Art 29 Working Party, ‘Opinion 02/2013 on Apps on Smart Devices’ (n 101).

106 Information Commissioner’s Office, ‘Principle (c): Data Minimisation’ <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to->

[the-general-data-protection-regulation-gdpr/principles/data-minimisation/](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/)> accessed 6 October 2021.

107 GDPR (n 4).

108 ICO, ‘Age Appropriate Design’ (n 20).

109 Centre for Information Policy Leadership (n 60).

110 EDPB, ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default’ (n 78); Lee A Bygrave, ‘Data Protection by Design and by Default: Deciphering the EU’s Legislative Requirements’ (2017) 4(2) Oslo Law Review 105.

Some authors criticize that PETs focus on the prevention of information disclosure instead of ensuring the protection of all GDPR principles and rights, which data protection by design is supposed to achieve.¹¹² They flag the focus of PETs on privacy-as-confidentiality as opposed to privacy-as-control (GDPR's approach). In this context, a recent study of the Siri voice assistant criticized Apple's approach. Apple's decisions are an example of embedding privacy into data management and software that has focused on what some have described as a 'rather narrow definition of privacy, which largely addresses confidentiality and data security.'¹¹³ It is certainly important for a company to explicitly state why it gives priority to data confidentiality over other GDPR rights that data subjects should normally be able to exercise. Rights and freedoms of the data subject need to be safeguarded.¹¹⁴ However, having said that, in some situations, limiting a data subject's rights could be an adequate solution if transparently explained, for example, through the publication of a DPIA. From the perspective of a vulnerable person's needs and considering GDPR's provisions on the necessity to adopt special protection measures in relation to children¹¹⁵ and to tackle increased risks when vulnerable people's data are processed,¹¹⁶ Apple's approach of insisting on confidentiality over the possibility of exercising other data subjects' rights could be correct. Of course, if confidentiality and the exercise of other rights can both be achieved at a satisfactory level, then it should be done so. In any case, efforts should be made in this direction. While waiting for the appearance of such systems (which should be promoted and researched), this article considers that the confidentiality of a vulnerable person's data should be the top priority. If there are people able to effectively manage and protect their personal data, for children or some adults with disabilities the benefits of being able to exercise their right of access (for example) will probably not surpass the benefits of higher data confidentiality (if

exercising this right would result in the creation of higher data breach risks).

Protecting vulnerable people's data by default

Standard settings are crucial when evaluating the level of privacy offered by particular IoT devices as they determine how easy it is for users to apply the relevant configuration for a data protection compliant use of the product.¹¹⁷ It should be up to the data subject to decide whether they want to allow their personal data to be used in a broader manner.¹¹⁸ Vulnerable individuals might lack understanding or not be able to exercise informed control over their personal data. This is confirmed in recital 58 of the GDPR, which states that the justification for the protection of children is founded on their diminished capability of understanding (it should be noted that while recitals can help in the interpretation of ambiguous EU law provisions, they are not legally binding).¹¹⁹ There are important gaps in the development of children in terms of their comprehension of the digital environment in which their personal data are processed.¹²⁰ For example, in the case of persons aged 16–17 years, the UK's Information Commissioner's Office suggests to 'provide written, video or audio materials to explain what will happen to their information and any associated risks' if they attempt to change a default high privacy setting and to check with an adult if they have any concerns or don't understand what is being communicated to them.¹²¹ The ICO's report indicates how important those default settings are. It is crucial that data processing is left to the choice of each individual as much as possible. Unfortunately, this is not the reality at the moment and many IoT devices continue to transfer personal data to third parties without even informing the data subject about these activities.¹²²

This article argues in favour of adopting explicit opt-in mechanisms always and for everyone instead of differentiating between ordinary citizens and children or

111 Claudia Diaz, Omer Tene and Seda Guerses, 'Hero or Villain: The Data Controller in Privacy Law and Technologies' (2013) 74 *Ohio State Law Journal* 923.

112 Veale, Binns and Ausloos (n 52).

113 Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24(2) *International Journal of Law and Information Technology* 151.

114 GDPR, art 35.

115 *Ibid*, rec 38.

116 *Ibid*, rec 75.

117 Marit Hansen, 'Data Protection by Default in Identity-Related Applications' (IDMAN 2013: Policies and Research in Identity Management, London, April 2013) <https://link.springer.com/chapter/10.1007%2F978-3-642-37282-7_2> accessed 6 October 2021.

118 EDPS, 'European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the Data Protection Reform Package'

(2012) <https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf> accessed 6 October 2021.

119 Malgieri and Niklas (n 13).

120 Eva Lievens and Simone van der Hof, 'The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR' (2018) 23(1) *Communications Law* 33.

121 ICO, 'Age Appropriate Design' (n 20).

122 Ren Jingjing and others, 'Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach' (IMC '19: Proceedings of the Internet Measurement Conference, Amsterdam, October 2019) <<https://dl.acm.org/doi/10.1145/3355369.3355577>> accessed 6 October 2021.

vulnerable adults. In its Age Appropriate Design report, the ICO requires organizations to adopt ‘high privacy’ by default, to switch geolocation and profiling off by default ‘unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child’.¹²³ Some authors also stated that in the case of minors using a service, ‘default settings have to be especially strict’.¹²⁴ This is problematic for several reasons. First, organizations could argue that because their smart products are directed towards the general population, their default settings do not have to be as protective as for products that only children use. Adopting ‘high privacy’ default settings by default for everyone would not only make all citizens’ data safer, but also make sure that when it is uncertain whether a product is used by children (or vulnerable adults), default privacy settings would protect them anyway in case they are using it or decide to use it later. Secondly, the ICO mentions compelling reasons for a different default setting than a high privacy one, without giving examples of what could justify deviating from the GDPR provisions and spirit. This article argues in favour of making no such exceptions. Until proven to the contrary, it is difficult to envisage a situation in which a high privacy default setting should not apply. Thirdly, and relevant to the first two points, the ICO states itself that a lot of children will simply ‘accept whatever default settings you provide and never change their privacy settings.’¹²⁵ This article argues that this will also be certainly true in many cases for vulnerable adults. For this reason, it is of utmost importance to implement high privacy settings by default for every data subject to make sure that all vulnerable individuals are protected. Moreover, making individuals change their privacy settings if they want their data to be processed for a specific purpose would also educate them about personal data processing in the IoT world (as they would need to take active steps and think about their choices), thereby contributing to compliance with other GDPR provisions such as the transparency principle.

High risks of processing vulnerable people’s data and DPIAs

A DPIA’s objective is to evaluate, identify, and minimize risks related to a data processing activity before the latter takes place. According to Article 35.1 of the GDPR, a DPIA is required when a specific processing plan or

project is likely to cause a high risk to the rights and freedoms of individuals. Article 35.3 describes three cases in which a DPIA is always required (‘systematic and extensive profiling with significant effects’, ‘large-scale use of sensitive data’, ‘public monitoring’) and the ICO published a document in line with Article 35.4 listing 10 more examples.¹²⁶ Some activities among the latter require a DPIA automatically while others need to occur in combination with one of the criteria in the European guidelines (the WP29 lists nine other criteria). Processing activities on the basis of data gathered by innovative technologies is one of the ICO’s criteria that needs to be combined with one of those listed by the WP29. Therefore, the first question in the context of this article is whether smart devices can be considered as innovative technologies. Recital 91 mentions innovative technologies as developments in the technological field globally. The ICO considers that smart technologies (including wearables) fall into this definition.¹²⁷ As a result, IoT products fall into the ‘innovative technologies’ criteria of the ICO. The second question is whether this can be combined with one of WP29’s examples of situations likely to result in a high risk. For the WP29, processing data of vulnerable people is an indication that there could be a high risk involved. There is an inherent high risk when vulnerable data subjects’ data are processed as there is a power imbalance between the latter and the data controllers, in the sense that vulnerable people (such as children or vulnerable adults) might be incapable of easily consenting or objecting to the processing of their data, or exercising their rights.¹²⁸ In conclusion, smart devices (ICO’s innovative technology criteria) used by vulnerable people (WP29’s processing of vulnerable people’s data criteria) represent a situation that might result in high risks and, therefore, a DPIA will always need to be carried out.

DPIAs were not mandatory at the time of the Data Protection Directive. The obligation to carry out DPIAs in certain circumstances has been introduced by the GDPR. Obligatory impact assessments are not purely prescriptive legal regulations but rather a mix of legal requirements as well as policies that organizations need to develop and implement themselves (with the involvement of relevant stakeholders).¹²⁹ One author has described the term ‘co-regulatory’ as inadequate and lacking precision in defining what DPIAs are.¹³⁰ Instead, he proposes to use the notion of ‘meta-

123 ICO, ‘Age Appropriate Design’ (n 20).

124 Hansen (n 117).

125 ICO, ‘Age Appropriate Design’ (n 20).

126 ICO, ‘When Do We Need to Do a DPIA?’ (n 8).

127 Ibid.

128 Art 29 Working Party, ‘Guidelines on Data Protection Impact Assessment (DPIA)’ (n 9).

129 Reuben Binns, ‘Data Protection Impact Assessments: a Meta-Regulatory Approach’ (2017) 7(1) *International Data Privacy Law* 22.

130 Ibid.

systems that allowed cybercriminals to distort or damage them and burglaries that happened as a result of compromised smart locks, there are many security issues that vulnerable people might have to face if they live within a smart home.¹⁴⁰ For example, in 2015, the company Mattel created an IoT product, the Hello Barbie doll, which has the capacity to listen and talk with children. This toy is equipped with a microphone which records children's voices and transfers them to third parties for data analysis. The doll was easily hacked by a researcher who gained access to the device's files (including audio recordings) and was able to use the doll's microphone.¹⁴¹ Similarly, another doll named Cayla was accused by German authorities of spying on smart home members and sending the data it gathered to the USA.¹⁴² Finally, another example is the hacking of Vtech, a company producing digital baby monitors compromising information of more than 5 million customer accounts and children profiles, or the many stories of hackers accessing digital baby monitors and talking with infants through them.¹⁴³ These devices endanger vulnerable users and lead to GDPR compliance issues by undermining the security of consumers' personal data.

With the establishment of the 'integrity and confidentiality' principle, Article 5 of the GDPR has raised the act of ensuring data security from a simple requirement to one of the main data protection principles.¹⁴⁴ Ensuring the security of data is a prerequisite for lawful data processing, Article 4 (12) of the GDPR states that a data breach is a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.' Those processing activities of deleting, disclosing, or accessing data are not as such illegal.¹⁴⁵ If the controller is found to have taken relevant security measures and to not

have been negligent, the data breach will be considered accidental.¹⁴⁶ If, however, appropriate data protection safeguards are not implemented and a data breach occurs as a result, this would be a clear violation of the integrity and confidentiality principle and it would make the use of any legal basis unlawful. This is evaluated on a case-by-case basis.¹⁴⁷ Over the last few years, it has been proven that hackers were able to use Amazon Alexa and Google Home smart assistants in order to spy on data subjects without their knowledge, or to deceive them into giving sensitive personal information.¹⁴⁸ This has happened several times even though Amazon and Google have deployed countermeasures after each attack. Vulnerable people cannot be expected to understand when an IoT device is behaving in an unusual manner and to spot a data security threat. Those devices should ensure that security measures are sufficiently strong. While a data breach can theoretically always happen, the fact that it does over and over again is a worrying sign. In this case, would authorities consider the data breach as accidental? If countermeasures adopted by Google and Amazon are regularly proven ineffective over relatively short periods of time then the answer should probably gravitate towards a negative response (especially considering the resources at the disposition of those companies).

This article would also like to draw attention to the importance of standards for GDPR compliance with the integrity and confidentiality principle, and for the protection of vulnerable customers. Certification mechanisms can be given as an example. The objective of certification is to prove compliance with a group of standards. It can be described as 'conformity assessment' which serves 'to evaluate compliance of persons, products and/or processes with a given set of requirements.'¹⁴⁹ Labelling schemes have been recently put forward by the industry, certification bodies, and the government.¹⁵⁰ For example,

140 DCMS, 'Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report' (2018) <<https://www.gov.uk/government/publications/secure-by-design-report>> accessed 6 October 2021.

141 Samuel Gibbs, 'Hackers can Hijack Wi-Fi Hello Barbie to Spy on your Children' *The Guardian* (2015) <<https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children>> accessed 6 October 2021.

142 Forbrukerradet (Norwegian Consumer Council), '#Toyfail An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys' (2016) <<https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toy-fail-report-desember2016.pdf>> accessed 6 October 2021; Bouvet on behalf of the Norwegian Consumer Council, 'Investigation of Privacy and Security Issues with Smart Toys' (2016) <<https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf>> accessed 6 October 2021.

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

144 Ni Loideain (n 83).

145 Clifford and Ausloos (n 95).

146 Ibid.

147 Ni Loideain (n 83).

148 ZDNet, 'Alexa and Google Home Devices Leveraged to Phish and Eavesdrop on Users, Again' (2019) <<https://www.zdnet.com/article/alexa-and-google-home-devices-leveraged-to-phish-and-eavesdrop-on-users-again/>> accessed 6 October 2021.

149 ENISA, 'Security Certification Practice in the EU' (2013) <<https://www.enisa.europa.eu/publications/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study>> accessed 6 October 2021.

150 Shane D Johnson and others, 'The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay' (2020) 15(1) *PLoS One* 1.

preserving technologies can support legal compliance with those principles in the context of vulnerable people are needed). Only after this has been done as best as possible, should an organization evaluate what legal

basis to use if processing vulnerable persons' personal data is still required.

doi:10.1093/idpl/ipac001