Comments on the European Data Protection Board's

Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

Submitted by Prof. Derek McAuley, Dr. Ansgar Koene and Dr. Jiahong Chen of Horizon Digital Economy Research Institute, University of Nottingham

16 January 2020

1. Horizon[1] is a Research Institute centred at The University of Nottingham and a Research Hub within the UKRI Digital Economy programme[2]. Horizon brings together researchers from a broad range of disciplines to investigate the opportunities and challenges arising from the increased use of digital technology in our everyday lives. Prof. McAuley is Director of Horizon and Principal Investigator of the EPSRC-funded DADA[3] (Defence Against Dark Artefacts) project, addressing smart home IoT network security, and its acceptability and usability issues, the ESRC-funded CaSMa[4] (Citizen-centric approaches to Social Media analysis) project to promote ways for individuals to control their data and online privacy, and the EPSRC-funded UnBias[5] (Emancipating Users Against Algorithmic Biases for a Trusted Digital Economy) project for raising user awareness and agency when using algorithmic services. Dr Koene was a lead researcher of the CaSMa and UnBias projects, is Research co-Investigator on the EPSRC-funded ReEnTrust[6] (Rebuilding and Enhancing Trust in Algorithms) project and chairs the working group for developing the IEEE P7003 Standard for Algorithm Bias Considerations. Dr Jiahong Chen is a Researcher Fellow of Horizon, working on the DADA project.

Introduction

2. We welcome the EDPB's adoption of Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (DPbDD) and the call for comments on the current version, which have highlighted the importance of proper and effective implementation of DPbDD in ensuring a high level of data protection, and provided practical guidance for stakeholders.
3. The Guidelines have conducted a comprehensive analysis of Article 25 GDPR, and also the implications for compliance with data protection principles, and related certification and enforcement issues. We share the EDPB's observation that "[i]n an increasingly digital world, adherence to DPbDD requirements play a crucial part in promoting privacy and data protection in society", and agree with both the scope of the Guidelines and most of the interpretations of the relevant provisions. The aim of our comments is to contribute to the general approaches already reflected in the current version by pointing out the areas where the final version could further address. These points will be elaborated each in a section below and summarised in a conclusion,

[1] http://www.horizon.ac.uk

[2] https://epsrc.ukri.org/research/ourportfolio/themes/digitaleconomy/

[3] https://www.horizon.ac.uk/project/defence-against-dark-artefacts/

[4] http://casma.wp.horizon.ac.uk

[5] http://unbias.wp.horizon.ac.uk

[6] https://ReEnTrust.org

with several specific recommendations for the upcoming revision.

The role of "technology providers"

4. The Guidelines have picked up on Recital 78 GDPR with regard to the role of "producers of the products, services and applications" – a provision that we consider having profound implications but currently overlooked in the ongoing discussions. These technology providers do not necessarily qualify as data controllers or processors, but are playing an increasing role in determining the technical architectures in data processing systems. The Guidelines have rightly covered these actors.

5. We would however like to point out that the lines between the concepts of controllers, processors and technology providers can sometimes be unclear. This is particularly the case in areas where the technical configurations are complex and involves a variety of stakeholders, such as cloud computing, IoT and online advertising. While some players tend to argue they function simply as "facilitators" by providing the necessary infrastructures for data processing, in highly concentrated markets they may find themselves in a much more powerful position than the data controller, with the latter having very little actual choice or control over how personal data are handled. In the light of the expanding scope of "(joint) controller" interpreted by the CJEU,[7] the legal status of technology providers is not entirely clear. We noted it is part of the EDPB's Work Program 2019/2020 to update the Article 29 Working Party's Guidelines on concepts of controller and processor,[8] but for the purpose of the DPbDD Guidelines, it should also be emphasised that technology providers, who are merely "encouraged" to observe the data protection principles under the GDPR, should nevertheless take DPbDD seriously or even treat it as a legal requirement in the case of legal uncertainty.

6. What would also be significantly more helpful is to provide further examples of how technology providers may facilitate data controllers and processors to comply with DPbDD requirements. While the significance of technology providers has been clearly highlighted in Sections 1 ("Scope") and 6 ("Conclusions and recommendations"), it is not sufficiently covered by the legal analyses and examples given in the main sections.

Data minimisation and PETs

7. When explaining the factors to consider in determining the appropriate measures and safeguards (Section 2.1.3), the Guidelines have also stressed the need "to take account of the current progress in technology". It is indeed imperative for data controllers to consider carefully how the choice of technical approaches may have an impact on the effectiveness of fulfilling their DPbDD duties.

8. One development data controllers should keep a close eye on is privacy-enhancing technologies (PETs), which has been highlighted in the EDPS's 2018 Opinion on privacy by design.[9] Edge computing solutions and personal information management systems (PIMS), for example, can be useful architectural models for improving compliance with data protection principles, especially the data minimisation principle.[10] The prevalent cloud-computing model based on the "local-remote-

[7] See Jiahong Chen, Lilian Edwards, Lachlan Urquhart and Derek McAuley, "Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption". https://ssrn.com/abstract=3483511
[8] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf
[9] https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf
[10] Richard Mortier et al, "Personal Data Management with the Databox: What's Inside the Box?" Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking. https://doi.org/10.1145/3010079.3010082

local" data flows[11] is not always necessary and many of the data analysis tasks can be performed entirely on the data subject's devices/apps/browsers.

9. The EDPB may provide further regulatory incentives in the Guidelines by encouraging data controllers to shift to a technical model that relies less on centralised, cloud-based data collection and perform necessary data analyses on the user's terminal device as far as possible. It would be helpful to make it clearer that the design choice to keep data transfers to remote servers to a minimal necessity can contribute to the demonstration of the compliance with DPbDD requirements, as well as the data protection principles.

Dark pattern design

10. Another disturbing trend worth highlighting is the rise of dark pattern design, a kind of tactics whereby data subjects are tricked into granting permission to the use of their personal data.[12] These may include presenting information and options in such ways that data subjects would have a much stronger tendency to underestimate the risks or would have to make disproportionate efforts to opt out of unnecessary uses of their data.

11. We are of the view that such deceptive practices are contrary to *both* the data protection by design *and* by default obligations. By adopting a design pattern that unduly impedes the free choice of data subjects, the data controller would fail to fulfil their duty to "implement appropriate technical and organisational measures […] in an effective manner". Making it difficult for data subjects to choose not to have their personal data collected also amounts to enabling unnecessary data processing by default. In certain cases, this may even constitute a violation of the transparency principle, as well as the lawfulness principle, as the consent given via a manipulative UI cannot be considered "freely given" and thus cannot serve as a valid legal basis for the data processing in question.

12. We therefore see the need for the EDPB to reiterate in the Guidelines the incompatibility of dark pattern design with the letter or the spirit of Article 25 GDPR and the general data protection principles. Provision of information and obtaining individual consent must be carried out in a way that fully respects the free choice and autonomy of data subjects.

Conclusion

13. Overall, the EDPB's adoption of the Guidelines represents a helpful step forward in promoting ethical and privacy-friend design and default approaches, and the current version has largely covered right issues with an appropriate level of details and useful examples. To sum up the specific comments outlined above, we provide three recommendations as to how the Guidelines can be improved in the final version:

    - Throughout the Guidelines, make a stronger case for technology providers to fully align with the DPbDD requirements as imposed on data controllers, and provide further examples on how this can be achieved;

[11] Lachlan Urquhart, Tom Lodge and Andy Crabtree, "Demonstrably Doing Accountability in the Internet of Things" (2019) 27(1) International Journal of Law and Information Technology. https://doi.org/10.1093/ijlit/eay015

[12] Christoph Bösch, et al, "Tales from the dark side: Privacy dark strategies and privacy dark patterns" Proceedings on Privacy Enhancing Technologies. https://doi.org/10.1515/popets-2016-0038 Midas Nouwens et al, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence". https://arxiv.org/abs/2001.02479

- In Section 2.1.3 (“Elements to be taken into account”), specify certain PET approaches with examples that are already available and easy to implement for data controller to show better compliance with data protection principles;
- In Section 3 (“Implementing data protection principles […]”, in particular the “Transparency” and “Lawfulness” sub-sections), further clarify that data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.

14. We would be happy to be contacted for further discussion, and for our comments to be published.