Comments on the European Data Protection Board's

Guidelines 07/2020 on the concepts of controller and processor in the GDPR

Submitted by Prof. Derek McAuley, Prof. Lilian Edwards,
Dr. Lachlan Urquhart and Dr. Jiahong Chen of
Horizon Digital Economy Research Institute, University of Nottingham

19 October 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. Prof. Lilian Edwards is Professor of Law, Innovation & Society (Newcastle University) and Deputy Director of CREATe[6] (Centre for Creativity, Regulation, Enterprise and Technology), a UKRI-funded research centre focusing on copyright and business models. Dr. Urquhart is Lecturer in Technology Law (University of Edinburgh), Visiting Research at Horizon, and Co-Investigator of DADA. Dr. Chen is Researcher Fellow of Horizon, currently working on the DADA project.

Introduction

2. We welcome the EDPB's adoption of Guidelines 07/2020 on the concepts of controller and processor in the GDPR, as well as the call for comments on the current version, which addresses some of the most important and challenging legal issues under the current data protection regime.

3. The Guidelines have mainly focused on the definitions of data controller and data processor under the GDPR, and the relationships between the controller and the processor as well as between joint controllers, but also touched upon other relevant rules such as the principle of accountability. While we agree with the majority of the legal analyses conducted in the Guidelines, we would also like to, based on our research, point out certain specific issues for the Board to consider when finalising the Guidelines, especially the practical implications for data processing in a home context.

---

[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://www.create.ac.uk/

The role of "technology providers"

4. As highlighted in one of our previous submissions,[7] the legal status of "technology providers" are not entirely clear. This is especially the case when there is a clear imbalance of power and control between the technology provider and the end-user. In a (smart) home setting, for example, some devices are designed to collect personal data from within and/or outside the household, such as a smart doorbell. In these cases, both the purposes and means of data processing are pre-defined by the architectural design of the product, with the end-user controlling only whether and when the collection of data takes place.

5. The Guidelines touches on this scenario by discussing the cases of "platforms, standardised tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up." (para 63) This is further explained in Footnote 24 that "[t]he provider of the system can be a joint controller if the criteria mentioned above are met, i.e. if the provider participates in the determination of purposes and means. Otherwise, the provider should be considered as a processor." While this may largely apply to a business-to-business setting, it does not seem to reflect the actual circumstances in a typical business-to-consumer (or big-business-to-SME) reality, where the end-user (presumably as a data controller) has very little negotiating power over the technology provider. Where there is, for instance, a data breach due to the flawed design of the product, the end-user may even be unfairly held responsible as the sole controller. The power dynamics, in this regard, should also be factored into the ascertaining of data controllership.

6. Given the requirement for data protection by design and default (DPbDD) in Art 25, we also would like clarity on managing the power dynamics between joint controllers can be addressed with technical and organisational measures. There is need for greater clarity on the differentiation of responsibilities between vendors and domestic users in the home, and how they can satisfy their respective obligations. We would suggest the need for further investigation into new DPbDD tools that respond to the duality of shared responsibilities, enable compliance from the vendor perspective, but crucially, that would be usable for users to adopt in their domestic life.

Domestic data controllers

7. On the flip side, our analysis of the latest CJEU case law[8] has shown that, in the light of the narrowing scope of the household exemption, users of smart technologies may find themselves unable to be exempt from the GDPR on the basis of a "purely personal or household activity". They might well end up being held as what we call "domestic data controllers".[9] This gives rise to the question as to how accountability should be demonstrated by this category of data controllers, as well as how vendors of smart products should provide support to fulfilling this duty.

8. The Guidelines note that, "in line with the accountability principle, the use of a contract or other legal act will allow joint controllers to demonstrate that they comply with the obligations imposed upon them by the GDPR." (para 171) Again, although this would be a reasonable arrangement for entities who are able to negotiate their respective duties with regard to their roles in the joint controllership, it may end up shifting the compliance burdens to those who possess the least

---

[7] https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/comments_on_edpb_guidelines_on_a_25_dpbdd_-_horizon.pdf

[8] https://doi.org/10.1093/idpl/ipaa011; see also https://script-ed.org/article/between-a-rock-and-a-hard-place-owners-of-smart-speakers-and-joint-control/; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3570895

[9] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3629119

bargaining powers, especially when one of the joint controllers is a consumer. Following the stipulation of Article 26(2) as well as the logic of the Guidelines in establishing the existence of joint controllership (paras 47-50), we are of the view that the contract or legal act defining the responsibilities of the joint controllers should also reflect the actual influence exercised by each controller, particularly considering which controller is best-positioned to fulfil a specific duty. Examples covering these scenarios will also be significantly helpful.

Differentiated responsibilities

9. In the light of our comments above, the EDPB should also consider how to provide regulatory incentives to encourage joint controllers to come up with an arrangement that is fair both to the data subject (i.e. not impeding the data subject's exercising of their rights) and to the data controllers themselves (i.e. not over-burdening some of the joint controllers).

10. For example, the Guidelines note that, "[u]nder Article 26(3), a data subject is not bound by the terms of the arrangement and may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers." (para 184) While we agree that this is loyal to the text of Article 26(3), an alternative interpretation can be that, where the arrangement does not truly reflect the actual circumstances of the joint controllership, or where it creates additional burdens to the data subject, the data subject may exercise their rights against any of the joint controllers. Under this approach, the joint controllers, whether in a stronger or weaker position, would have the incentive to set out the mutual arrangement in a way that assigns the responsibilities to the best-positioned data controller (e.g. responding to right of access requests by the controller who has actual access to the data). This interpretation is also in line with the spirit mirrored in Article 82(3), where it is provided that a controller or processor may be exempt from the liability "if it proves that it is not in any way responsible for the event giving rise to the damage." Although this Article speaks of liability rather than a general responsibility, it is informed by the idea that, as the Board and the CJEU decisions have noted, responsibilities should be shared by joint controllers but not necessarily equally.

Conclusion

11. Overall, the EDPB's adoption of the Guidelines provides additional clarity and certainty for data controllers and processors to comply with the GDPR. To sum up the specific comments outlined above, we provide three recommendations as to how the Guidelines can be improved in the final version:

    - Further clarify the nature of the influence on the purposes and means of the processing exercised by the technology providers, especially when there is a clear power imbalance;
    - Explicitly specify that the arrangement between joint controllers as required by Article 26 should take into account which controller is best-positioned to fulfil a specific duty, ideally with real-life examples of domestic controllers;
    - Encourage joint controllers to agree on such an arrangement in a fair manner by allowing the arrangement to take effect on how data subject requests are handled, provided that it does not create any extra burden on the data subject.

12. We would be happy to be contacted for further discussions, and for our comments to be published in full.