Comments by Datenanfragen.de e. V. on the EDPB's "Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive"

Braunschweig (Germany), on January 17, 2024

Datenanfragen.de e. V. welcomes the EDPB's efforts to define guidelines on the technical scope of Art. 5(3) ePD, and wants to thank the members of the working groups for their work. We appreciate the opportunity to provide our comments on the guidelines from the perspective of a non-governmental consumer protection association.

Datenanfragen.de e. V. is a registered data protection non-profit based in Germany. Our primary focus is on helping data subjects exercise their data protection rights by providing tools and information to lower the barrier of entry and make the process as easy as possible. All of our tools are developed from the ground up with data minimisation in mind; wherever possible, processing is done locally on the user's computer and requests are sent by the user themselves, with no data ever reaching our servers.

Another part of our work is research and analysis of data protection practices primarily in the context of websites and apps. For example, we have done work on data protection violations and consent dialogs in mobile apps[1] and analysed the data safety labels on the Google Play Store[2] as well as the privacy labels on the Apple App Store[3].
Finally, we are running Tweasel[4], a project building infrastructure for detecting and complaining about tracking and privacy violations in mobile apps on Android and iOS. As part of this project, we developed a tool suite for automated app analysis and tracking detections.

Comments

In our work, we have unfortunately seen that Art. 5(3) ePD is often misunderstood or even ignored by website and app operators, despite having been in force for many years. As such, we are glad

[1] Koch et al., The OK Is Not Enough: A Large Scale Study of Consent Dialogs in Smartphone Applications, 32nd USENIX Security Symposium, https://www.usenix.org/system/files/usenixsecurity23-koch.pdf

[2] Altpeter, Worrying confessions: A look at data safety labels on Android, https://www.datarequests.org/blog/android-data-safety-labels-analysis/

[3] Koch et al., Keeping Privacy Labels Honest, Proceedings on Privacy Enhancing Technologies 2022 (4), https://petsymposium.org/popets/2022/popets-2022-0119.pdf

[4] https://docs.tweasel.org/

Datenanfragen.de e. V.
Schreinerweg 6
38126 Braunschweig
Deutschland

Eingetragen im
Vereinsregister des
Amtsgerichts Braunschweig:
VR 201732.
Als gemeinnützig anerkannt.

Fon: +49 531 209299 35
Fax: +49 531 209299 36
Mail: info@datenanfragen.de
Web: verein.datenanfragen.de

Spendenkonto:
Datenanfragen.de e. V.
DE42 8306 5408 0104 0851 40
GENODEF1SLR
Deutsche Skatbank

that the guidelines make the wide scope of Art. 5(3) ePD clear. We also welcome that the EDPB references the existing guidance of the WP29 on the subject.

We explicitly support these guidelines and the positions the EDPB takes. We especially want to voice our support for:

- The clear position that the protection by the ePD is not dependent on whether the communication was initiated by the user or even on whether the user is aware of said communication (para. 19).
- The clear position that making a network available to only a limited subset of the public does not make it private and thus does not preclude the applicability of Art. 5(3) ePD (para. 25).
- The clear position that the notions of "gaining access" to and "storing" information are independent of one another and do not need to be carried out by the same entity (para. 29).
- The clear position that information is considered to be stored on the terminal equipment of a user not only if a party has direct access, but also if the party instructs software on the terminal equipment to generate specific information, regardless of who created or installed the software or the protocols used (para. 35).
- The clear position that the ePD does not place any upper or lower limit on the length of time that information must persist on a storage medium to be counted as stored and that there is no upper or lower limit on the amount of information to be stored (para. 36).
- The clear position that "stored information" may not just result from information storage in a restrictive sense, but is also present if it was stored by any other entity (including the user or manufacturer) or if it was read from sensors (para. 39).
- The clear positions that tracking pixels and tracked URLs constitute storage on the user's terminal equipment (para. 50), and that the inclusion of such elements in the content sent to the user constitutes an instruction to the terminal equipment to send back the targeted information (para. 51).

Additionally, we have identified a number of subjects that we believe would benefit from additional clarification:

- Section 2.2 elaborates on the notion of "information", mentioning that it is intended to be a much broader concept than that of personal data (para. 7), and listing various factors that have no influence on whether something is to be considered "information" (para. 12). While we appreciate that this should be obvious from the word itself, we would welcome a more explicit definition or explanation of the word "information". In our work and research,

Datenanfragen.de e. V.
Schreinerweg 6
38126 Braunschweig
Deutschland

Eingetragen im
Vereinsregister des
Amtsgerichts Braunschweig:
VR 201732.
Als gemeinnützig anerkannt.

Fon: +49 531 209299 35
Fax: +49 531 209299 36
Mail: info@datenanfragen.de
Web: verein.datenanfragen.de

Spendenkonto:
Datenanfragen.de e. V.
DE42 8306 5408 0104 0851 40
GENODEF1SLR
Deutsche Skatbank

we have often encountered accessing entities who believed their accessing of information from a user's terminal equipment not to be covered by the ePD because they considered the information to be mundane. As such, we would suggest a clarification that the ePD has no such significance threshold and can really cover *any* information.

- The guidelines mention that Art. 5(3) ePD applies whenever the accessing entity wishes to gain access to information stored in the terminal equipment and actively takes steps toward that end (para. 31). We would appreciate additional clarification on cases where the terminal equipment automatically sends information without the accessing entity instructing it to (for example, browsers will typically always send a `User-Agent` header, with the server having no influence over that). Can such cases never be covered by Art. 5(3) ePD? Is there a difference in whether the accessing entity *actually* ends up accessing the information?
- The guidelines make mention of cases where the entity instructing the terminal to send back the targeted data and the entity receiving said information are not the same, but then only say that Art. 5(3) ePD "may still apply" without providing further details on when that is or is not the case (para. 33). Such situations are very prevalent in online tracking and we thus believe this to be a very relevant question that we would appreciate further clarification on. Additionally, we would appreciate clarification on which party is responsible for any potential violations that may occur in such situations.
- Dicussing the notion of "storage", the guidelines include a list of examples of types of storage mediums that Art. 5(3) ePD applies to. These examples are very focussed on traditional computers. Considering the relevance of mobile tracking and consumer IoT devices, we would suggest including a phone's flash storage as well as the EEPROM of a microcontroller as examples here to avoid misunderstandings.

Final remarks

We remain available for any questions the EDPB have. For questions regarding this statement, please contact the association's board at `vorstand@datenanfragen.de` (PGP key `2E72 EA5B DDE3 1730 58D7  F87D A0C1 C012 3E2B 296B`).

Datenanfragen.de e. V.
Schreinerweg 6
38126 Braunschweig
Deutschland

Eingetragen im
Vereinsregister des
Amtsgerichts Braunschweig:
VR 201732.
Als gemeinnützig anerkannt.

Fon: +49 531 209299 35
Fax: +49 531 209299 36
Mail: info@datenanfragen.de
Web: verein.datenanfragen.de

Spendenkonto:
Datenanfragen.de e. V.
DE42 8306 5408 0104 0851 40
GENODEF1SLR
Deutsche Skatbank