

No. 2024-K-0111.3

Subject: opinion on Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

Vilnius, Lithuania, 2024 January 11.

Dear Colleagues,

After reviewing of "Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive" (Guidelines in this text below) and discussion with the professionals in personal data protection field, please find suggestion and proposals below for the further consideration.

1. SUGGESTIONS FOR CHAPTER 2.1 OF GUIDELINES (NOTION OF INFORMATION)

Information which allows effective tracking of user may be stored for secondary purposes and may not be stored in "terminal equipment". Such scenarios deserve additional clarification. For example, analysis of log files may equal effective user tracking, as in many cases logs are reflecting details user activity even without of use of cookies or other digital fingerprinting techniques. Also, log's may be stored in different location and by different application (such as ICT security equipment).

Proposal: to include in this chapter reference to secondary information collected during user activity

"access to of secondary information, such as log files with the purpose of user tracking also constitute tracking activity, not dependent where, how and by which technical means such information is collected". Use of security logs for dual purposes may constitute tracking as well.

2. VIRTUAL AND CLOUD ENVIRONMENTS INCLUSION (CHAPTER 2.3 OF GUIDELINES)

Notion of "Terminal Equipment" in this specific context is limiting and may not correctly reflect scope of current ICT (Information and Communication Technology) developments.

With broad expansion of various cloud services, extensively used by users there are broad range of technology solutions which may use cloud computing as main media for information storage and processing. Some examples include, but are not limited to:

- Virtualized workplaces in the cloud (computer or server which may fully replicate usual desktop or notebook computer of user);
- Virtualized "containers" running various software for user;
- Cloud services for specific user which may have modifiable information or possibility to store tracking information;





- Various public services in cloud which are used as main or supplementary information storage (e.g. Google Workspace, Microsoft OneDrive or Sharepoint, Dropbox, etc.) and are supplementing (or fully replacing) local storage in computer, tablet device or smartphone;
- Terminals which assure only input and output (visualization) of information, but do not have any local storage and processing;
- Agents (software modules running for specific user in cloud or locally);

Mentioned cloud and virtualization technologies may create a ambiguity in current Guidelines allowing circumvent current tracking limitations due to limiting definition of "terminal equipment". For example, technically there is an easy way to do all user tracking with the cookies or any other digital fingerprinting techniques storing information in personal account in cloud without any interference with "terminal equipment" according it's current definition. Current explanation in paragraph 16 of Guidelines "A terminal equipment may be comprised of any number of individual pieces of hardware" do not fully reflects cloud computing scenario's.

<u>Proposal</u>: update paragraphs 16 and 18 of current version of Guidelines with wording marked below with <u>underline</u> clarifying equivalence of operations and tracking in cloud and physical devices:

- 16. A terminal equipment may be comprised of any number of individual pieces of hardware and/or software, which together form the terminal equipment. This may or may not take the form of a physically enclosed device hosting all the display, processing, storage and peripheral hardware (for example, smartphones, laptops, connected cars or connected TVs, smart glasses). Terminal equipment may include virtualized instances of hardware and software, cloud services such as user accounts which may store information in similar manner as physical hardware devices. Such services and devices may not be directly accessed by users, but can be operated through electronic communication network.
- 18. The user or subscriber may own or rent or otherwise be provided with the terminal equipment including various digital services equivalent to terminal equipment. Multiple users or subscribers may share the same terminal equipment in the context of multiple communications (for example, in the case of a connected car) and a single communication may involve more than one terminal equipment.

3. NOTION OF "STORAGE" (CHAPTER 2.6)

Storage in the cloud computing context may be virtualized and distributed. As paragraph 37 enlists different types of storage in detail, suggestion here would be also to include notion of virtualization to include scenarios where information may be distributed even without user's knowledge about specific location of his/her information.

Proposal: update paragraph 37:

37. Similarly, the notion of storage does not depend on the type of medium on which the information is stored and ways how storage medium operates. Typical examples would include hard disc drives (HDD), solid state drives (SSD), flash drives and random-access memory (RAM), but less typical scenarios involving a medium such as magnetic tape or central processing unit (CPU) cache are not excluded from the scope of application. The storage medium may be connected internally (e.g. through a SATA connection), externally (e.g. through a USB connection) or through a network protocol (e.g. a network-attached-storage device). Storage may be virtualized, physically and geographically distributed. Storing of tracking information may should be considered in it's entirety even in those cases where such information may be distributed across different datacenters.



Allow me to convey our appreciation for opportunity to express opinion regarding Guidelines.

Respectfully,

/ signed by e-signature /

Martynas Bieliūnas, CIPP/E, CIPM, ISO27001 Lead auditor Managing Partner, member of LDAPA (Lithuanian Data Protection Officers Association) board

Smolensko str. 10B, LT-03201, Vilnius, Lithuania Mob.: +370 698 25292; Ph. +370 5 254 8240

E-mail: martynas@privacypartners.lt

https://www.privacypartners.lt