LEWIATAN

Warszawa, 7 marca 2019 r.
KL/101/45/AM/2019

Pan
Marek Zagórski
Minister Cyfryzacji

Szanowny Panie Ministrze,

W związku z publikacją na stronie podmiotowej Rady UE najnowszej wersji projektu *rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE,* zaproponowanej przez Prezydencję Rumuńską (dokument nr 6771/19 z dnia 22 lutego 2019 r.), Konfederacja Lewiatan, w załączeniu, przesyła stanowisko do projektu.

Mając na uwadze dotychczasową, bardzo udaną współpracę z resortem cyfryzacji w ramach prac nad projektem rozporządzenia, wyrażamy nadzieję, że uwagi Konfederacji Lewiatan spotkają się z Państwa przychylnością w toku dalszych prac nad projektem.

Z poważaniem,

Henryka Bochniarz
Prezydent Konfederacji Lewiatan

Do wiadomości:
- **Pani Wanda Buk** - Podsekretarz Stanu, Ministerstwo Cyfryzacji
- **Pani Agnieszka Krauzowicz** - Dyrektor Departamentu Telekomunikacji, Ministerstwo Cyfryzacji

Załącznik:
Stanowisko Konfederacji Lewiatan odnoszące się do projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (dokument nr 6771/19 z dnia 22 lutego 2019 r.).

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

Stanowisko Konfederacji Lewiatan odnoszące się do projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (dokument nr 6771/19 z dnia 22 lutego 2019 r.)

1. First, a high level of legal uncertainty remains when legal entities (companies) are in the scope of the e-Privacy regulation. From our view it is not clear from the text of the proposed regulation, when a company can consent to the usage of electronic communication services which are needed for business purposes. It is also highly unclear, when a company can decide on updates on business software, e.g. on tablet computers which are needed to control production lanes, or business apps on smart phones of the employees.
   Here it should be clear that companies (employers) should in a job-context be the 'end-user' who gives consent to ECS which are needed for the business and decides on updates on terminal equipment which is needed for job-purposes. Otherwise communication services and software would not reflect the needs of companies, and severe security threats would arise.

2. Recital 19b

   (19b) Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal entity subscribed to business-related electronic communications services**, for instance for the professional communication of employees.** ~~may allow a natural person, such as an employee, to make use of the service.~~ In such case, consent **may** ~~needs to~~ be obtained from the **legal person concerned, and not necessarily from the individual user.** ~~the individual concerned.~~

   Justification

   If electronic communication services are used to carry out business-related (non-private) communication of a legal entity, the consent must be obtained by the legal person or a competent individual acting on behalf of the legal entity. This can also be the individual end-user, if the legal person decides to delegate the consent in general, for specific services or in individual cases to a natural person (for example the employee)

3. Recital 20a – proposal for a deletion of the recital:

   a) Proposal for white list remains centered around browsers;
   b) Proposal will be complicated to implement. Today, we have no guarantee that internet browsers and OS will be able to implement such systems allowing browsers to connect with service providers.
   c) Proposal does not offer context for consent (i.e. we cannot explain why we request consumer consent) which is critical.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

4. **23a) Terminal equipment which is used for business reasons, such as computer, laptops, tablet computers or smart phones, for example to control production facilities and machines or to run business software, has to be automatically updated, maintained and managed to reflect the relevant business needs and to comply with information security requirements. In this context, the end-user is the legal person (employer), for example a company, who must give consent to the use of processing and storage capabilities of terminal equipment and the collection of information from terminal equipment.**

   Justification

   To provide a high level of IT security, updated software and apps reflecting the business needs and processes of a company, the consent for data processing with regards to terminal equipment must be obtained by the legal person (employer) or a competent individual acting on behalf of the legal entity. This can also be the individual end-user, if the legal person decides to delegate the consent in general, for specific services or in individual cases to a natural person (for example the employee).

5. Art. 4 (2) – the latest Council text states that for the purpose of this Regulation "processing" referred to in Article 4(2) of GDPR shall "not be limited to processing personal data". This is not clear how such extension relate to the clear scope restriction to "personal data" in Article 1 (1) of the Regulation.

6. Art. 6 - although there have been improvements made in Art. 6 which to some extent align processing of electronic communication data with GDPR, there are still some concerns which should be addressed:

- Art. 6(2a, last sentence) which allows processing only when it does not lead to user profiling should be complemented in a way that would further align it to the risk-based approach of Art. 22(1) GDPR in order to both achieve legal certainty and focus on what directly affects the privacy of end-users. Therefore it should be reworded in the following way: *"the electronic communications metadata is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user* ***which produces legal effects concerning him or her or similarly significantly affects him or her****".*

- Art. 6(2)f – The requirement that processing for statistical purposes is only allowed if based on EU or Member State law may jeopardize harmonized approach of the Regulation. Processing of metadata for statistical purposes should follow the logic of Art. 5(1)b GDPR.

- In our opinion a new legal base should be added in Art.6 (2): ***"it is necessary for compliance with a legal obligation"***
  This would make e-Privacy regulation more future proof. It cannot be excluded that Union law in future will impose on undertakings obligations that would make processing of communications metadata necessary. This would also be consistent with Art. 6 (1) c GDPR (processing is necessary for compliance with a legal obligation to which the controller is subject).

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

7. Art. 7(2)

Art. 7 (2) imposes on undertakings an obligation to erase metadata or made it anonymous when it is no longer needed for the purpose of the transmission of the communication. Exceptions are foreseen only in Art.6(1) b (security and technical faults), Art.6(2) a (mandatory quality of service) and Art.6(2) c (user consent). This provision should not lead to the obligation to delete the content or metadata immediately after transmission, if there is a legal ground to use metadata under Art. 6. For example, it is permitted to detect fraudulent use under Art. 6(2)(b), but fraud detection is not covered by list of exemptions from Art.7(2). This would result in the obligation to immediately erase the data after transmission of communication which would hinder providers to successfully detect fraudulent use. It should be noted that the GDPR already foresees that personal data can only be used to fulfil the purpose of processing. Once the purpose has ended, personal data can no longer be processed.

8. Art. 4a(3)

We suggest to delete the obligation provided for in Art. 4a(3) to remind end-users about their right to withdraw their consent every 6-12 months. GDPR already gives data subjects the right to withdraw consent at any time, even in the context of processing special categories of data (Art. 9 GDPR). Such obligation will not only create regulatory uncertainty for undertakings but will also lead to consent-reminder fatigue for the end-users.

9. Art. 8 (2)

Art. 6 largely relates to processing of metadata in connection with the provision of an electronic communication service, while Art. 8 regulates the collection and processing of metadata via terminal equipment. In our opinion Art. 8 should not apply to the 'standard' provision of an electronic communication service. We recommend to clarify that the conditions set forth in Art. 8(2) do not cumulate with Art. 6(2) for the processing of metadata by telecommunications providers. Otherwise, the Regulation would make an artificial distinction between metadata in general and those metadata emitted to enable the end-user's terminal to connect to the network.

10. Recital 12

E-privacy should not cover M2M communication when it relates to industrial processes. The focus of the ePR should be to protect the confidentiality of communications of natural persons. For the protection of natural persons with regard to the processing of their personal data, the GDPR already sufficiently covers the IoT environment. Moreover, the Regulation should apply only to the transmission of machine-to-machine communications containing personal data and only to the extent necessary to protect the confidentiality of communications (connectivity layer).

KL/101/45/AM/2019

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS