Spolek pro ochranu osobních údajů

Comments on the EDPB's draft "Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive"

We welcome the opportunity to present our comments to the recently published EDPB draft of Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive (Guidelines).

We appreciate the effort of the EDPB to provide opinions and recommendations on the Art. 5(3) of ePrivacy Directive.

General comments

1. We believe that in some respects the EDPB's interpretation clearly exceeds the bounds of the legislative text and intention. In particular, it is an interpretation that applies the rules of Article 5(3) ePrivacy to those cases where the processing of information emitted by an terminal equipment is involved, irrespective of whether the information is emitted on the basis of an 'instruction' from the user (e.g. by filling in a form) or within the technical characteristics of the network. It is clear from the text of Article 5(3) ePrivacy and its rec. 24 (as indeed the EDPB itself suggests) that the legislator's intention was indeed to protect the private sphere of the individual (including the legal person). Although, of course, in the case of information emitted to communication networks by terminal equipment (without being initiated by third parties), it cannot be ignored that this is information that will still be protected by law (e.g. under telecommunication secrecy, or GDPR if personal data is involved), it is no longer information that remains entirely in the private sphere of the person concerned and the application of the ePrivacy Directive should thus only be made where the circumstances actually justify it. Moreover, they do not meet the basic conditions of 'gaining access' or 'storing information' (see below).

   There is no justification for applying ePrivacy to cases where information is emitted directly by devices in this way, be it because of the intention of the user or the technical settings of the network environment. We do not consider such an extension of the application of the ePrivacy Directive beyond the control of the legislator by mere guidance from supervisory authorities to be both fortunate and permissible.
   Of course, as stated above, this does not mean that such information would be without legal protection, especially where personal data is involved, under the GDPR. However, it is also protected and regulated by other legislation, some of it quite recent, e.g. under the currently adopted Data Act.

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

2. While we understand the EDPB's intention to address only part of the interpretation of Article 5(3) of the ePrivacy Directive, we would like to point out that there are a number of other unclear issues related to this Article. These may include questions such as:
   a. the interpretation of the exceptions to the consent requirement under Article 5(3)
   b. the role of the various actors in the case of an end-user device provided to an employee by the employer. Here, a number of issues arise also with regard to the data protection of legal persons (which, as the EDPB rightly points out, are also covered by ePrivacy), as the individual's decision is always at the end anyway.

   We would very much appreciate it if the EDPB would also comment on these issues, which are very relevant in practice, in the context of this document or in the future.

3. Considering that the opinion interprets terms used in other legislation, such as Directive 2018/1972, we believe that it would be appropriate to prepare this opinion as a multidisciplinary opinion in cooperation with the bodies associated in BEREC.

Specific comments

Point 6 of the Guidelines.

Following the above mentioned remarks, we note that criteria B and D in this section also make it clear that the ePrivacy Directive cannot be applied to data objectively and without the involvement of a third party (who would be motivated to initiate its use) emitted by the device. This does not mean that such information would remain unprotected, but its protection is (as long as it is personal data) sufficiently ensured through the GDPR.Point 15 of the Guidelines.

Here, we would recommend emphasizing that even if such cases are not covered by ePrivacy, they may be regulated by other regulations (such as GDPR, other ePrivacy provisions or other telecommunications confidentiality regulations).

Point 25 of the Guidelines.

We would appreciate more examples where the EDPB does not consider a telecommunications network to be public. These examples could be defined in cooperation with BEREC.

Point 41 – 43 a body 51, 55 a 59 of the Guidelines.

As highlighted above, in our view a distinction should be made between information processed (stored) in the device and information "emitted by the device". We agree on the one hand with the EDPB's view that " *Use of the words "stored or accessed" indicates that the storage and access do not need to occur within the same communication and do not need to be performed by the same party.*" (see point 6 of the Guidelines). On the other hand, if the device is actively transmitting information to the communication network without being triggered by a third party (regardless of whether it is doing so on the basis of an "instruction" from its user or as part of the technical characteristics of the network), then we do not consider that Article 5(3) applies to this information in any event, because here no person is actively gaining access to this information by his or her actions ("gaining access").

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

In our view, this Article should only apply if the transfer is deliberately induced by a third party (even if it is subsequently used by another person distinct from the third party). The case where this information would be emitted by the device itself as a consequence of its manufacturer's setting without being necessary for its proper functioning, which may be the case for example for some IoT devices (see also point 59 of the Guidelines), is questionable from a legal point of view.

We believe that the text of the ePrivacy Directive does not allow for a different interpretation and in this respect the EDPB's views go beyond the legislative text in our view. A clear example of such an extensive interpretation that goes beyond the intention of the legislator may be the text of point 62 of the Guidelines: " *As outlined before, the fact that the information is being inputted by the user would not preclude the application of Article 5(3) ePD with regards to storage, as this information is stored temporarily on the terminal before being collected.*". If we understand the intention of the EDPB correctly, then the "sending" of any information from a terminal equipment, for whatever reason and at the instruction of anyone (including the user of that equipment), would then trigger the application of Article 5(3), as such information would first "have to be stored on the equipment". However, such a view has no basis in the text of the Directive and would amount to a complete change of interpretation and an unjustified extension of the ePrivacy Directive's impact. The Directive is intended to tighten protection for specific cases of intrusion into privacy, not to create a requirement for consent as the sole legal basis for processing for almost all information moving on the internet. We address this point in more detail below.

Point 47 a 51 of the Guidelines.

We agree that if the sender actively adds a tracking pixel to the email, the ePrivacy Directive will apply. We note, however, that similar data to the tracking pixel can be obtained in the case of secondary use of ordinary email content (e.g. ordinary images and information about their download). In such a case, it is questionable whether this case is regulated by Article 5(3) of the ePrivacy Directive or "only" by the GDPR.

Points 61 to 63 of the Guidelines.

We believe that the current wording of these points extends the application of the ePrivacy Directive beyond its statutory wording and may conflict with data protection or anti-spam principles. We consider the most problematic, as noted above, to be the sentence:
"As outlined before, the fact that the information is being inputted by the user would not preclude the application of Article 5(3) ePD with regards to storage, as this information is stored temporarily on the terminal before being collected."

Our understanding of this interpretation is that it is not possible to collect data entered by the user when visiting a website (e.g. when registering an account or signing up for a newsletter) without the user first consenting to optional cookies (unless an exception under Article 5(3) of the ePrivacy Directive applies). The application of the ePrivacy Directive is inferred by the EDPB from the fact that before the user sends data to the website operator, the data is temporarily stored on the user's terminal device.

This interpretation is problematic for two reasons. First, this interpretation is not consistent with the wording of Article 5(3) of the ePrivacy Directive. This Article cannot apply to data that is emitted by the user (whether on his instructions or according to network settings). More on this argumentation above.

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

Second, we believe that such an application could also conflict with Article 13 of the ePrivacy Directive and with other regulations, in particular the GDPR.

GDPR

The processing of data entered directly by the user may have a separate legal regime under the GDPR, which does not necessarily correspond to the regime under Article 5(3) of the ePrivacy Directive. For example, if a user consents to receive a newsletter and fills in their email address, it could be inferred from the proposed guidelines that they must have previously consented to optional cookies at the same time, as the provided email address was temporarily stored on their end device.

Theoretically, it could be argued that sending the newsletter and the associated storage of the information entered by the user would fall within the exception of Article 5(3) of the ePrivacy Directive, as it is necessary to provide a service that the user has explicitly requested. However, then the legal title for the processing would not correspond - under the ePrivacy Directive it would be legitimate interest, and under the GDPR consent.

Until the EDPB provides further explanation on this matter or clarifies the context, this wording will raise a number of questions and interpretative issues. „Simultaneously, we are convinced that clear guidance from the EDPB on this set of questions and issues is very important, in particular due to other upcoming regulatory acts or self-regulatory activites (e.g. the Cookie Pledge or the limitation of the usability of third-party cookies by browsers with the most significant market share announced to become effective later in 2024).

Art. 13 of ePrivacy Directive

Another example is when a user enters their details into an account registration form. Typically, this data is collected by an information society service provider for user authentication, account creation and service provision. In most cases, such processing takes place on the basis of Article 6 (1) (b) GDPR, i.e. for the performance of a contract with the data subject. Therefore, even here, the legal title for the collection of data would not necessarily correspond if the ePrivacy Directive were to apply.

In addition, marketing communications may be sent to the registered user as a customer of an information society service provider on the basis of Article 13 (2) of the ePrivacy Directive. Here, the ePrivacy Directive exemption would not apply because it would not be a service that the user has explicitly requested. Moreover, the so-called customer exception does not require the collection of consent. If the wording as proposed by the EDPB were to be applied, it would mean that a website provider would not be able to send marketing communications to its own customers unless the users have first given their consent to optional cookies.

Overall, the application of such an interpretation would mean that the website provider would not be able to process in any way the personal data entered by the user unless an exemption applies or the user has given consent to optional cookies. In practice, this would mean that the user could in many cases be prevented from interacting with the site at all, which would be fundamentally restrictive. Such an interpretation was certainly not the intention of the legislator when drafting the ePrivacy Directive.

The vast majority of website providers operate on the assumption that data specifically entered by the user as part of a customer account is not subject to the ePrivacy Directive regime.

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

Changing this principle in practice will undoubtedly raise a number of issues and questions. It would therefore be appropriate for the EDPB to consider the wording of these points and provide additional clarification and contextualisation with practical examples.

We are grateful for the opportunity to provide our comments on the draft Guidelines.

Prague, 17.1.2024

JUDr. Vladan Rámiš, Ph.D., Chairman of the Committee
Mgr. Jana Pattynová, LL.M., Member of the Committee
JUDr. Ing. Jindřich Kalíšek
Spolek pro ochranu osobních údajů

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562