Contribution to the EDPB's guidelines on the technical scope of Art.5(3) of the ePrivacy Directive

January 2024

AFEP member companies welcome the opportunity to take part to the public consultation opened by the European Data Protection Board (hereinafter referred to as "**EDPB**") on its draft guidelines 2/2023 on the technical scope of Article 5(3) of ePrivacy Directive (hereinafter referred to as "**ePD**"). AFEP member companies believe that a lack of legal certainty exists on this subject.

Companies note that a very broad interpretation of the technical scope of Article 5(3) of ePD is adopted by the EDPB. Such interpretation goes far beyond the letter and spirit of the ePD and may cause undue burdens to organisations and individuals alike (**1**).

AFEP member companies have also identified certain shortcomings and ambiguities that need to be addressed before the adoption of a final version, mainly relating to the following points: the notion of "*equipment*" (**2**); the notion of "*electronic communications network*" (**3**); the notion of "*gaining access*" (**4**); the notion of "*stored information*" and "*storage*" (**5**); and use cases relating to URL and pixel tracking (**6**).

1. General comments

AFEP member companies question the EDPB's competence to adopt these guidelines as the ePD also covers non-personal data that fall outside the scope of the GDPR and not in the remit of the EDPB's competences under the GDPR. In addition, only 12 national data protection authorities (out of a total of 27 in the EU) are competent to ensure the implementation of the ePD. Other national authorities designated to implement the ePD are not represented in the EDPB, and as a consequence, these draft guidelines cannot represent their views. Moreover, as the ePD has already been transposed into the national laws of the 27 Member States, with possible divergences as permitted by a Directive, the EDPB approach risks bringing more confusion and legal uncertainty than harmonisation.

In addition, AFEP member companies question the timing of these guidelines where the whole Internet already risks to be destabilized by the announced end of third party cookies by Google in 2024. These guidelines add more complexity to an already very uncertain landscape. With little visibility at this stage on what will come out of the Google privacy sandbox that should propose solutions to replace third-party cookies after the testing period, the EDPB narrow interpretation risks favoring Google in the end to the detriment of EU innovative actors.

Companies would first like to point out that the draft guidelines contain uncertainties or imprecisions that should be clarified by the EDPB.

1.1. Indicating that criteria A to D are cumulative

First of all, the EDPB starts its analysis by stating that Article 5(3) of the ePD should apply if four criteria, listed A to D, are fulfilled (§6). AFEP member companies understand these criteria as being cumulative, as for example, Article 5(3) should not apply if the operations carried out do not involve a "*terminal equipment*". For the sake of clarity, the guidelines should therefore indicate that these criteria are cumulative.

Moreover, the Guidelines do not provide any insight on the interpretation of the notion of "*user*", as well as on its importance when it comes to determining the application scope of Article 5(3). Pursuant to Article 2(2), a "***user***" is "***<u>any natural person using a publicly available electronic communications service</u>****, for private or business purposes, without necessarily having subscribed to this service*". It seems therefore important to consider this definition when assessing the applicability of article 5(3). It may also be useful to clarify what "*using a publicly available electronic communication service*" means. In any case, if the relevant individual is not using a publicly available electronic communication service, then Article 5(3) cannot/should not apply with respect to that specific individual.

1.2. Absence of guidance on exemptions

The EDPB specifies that the "*guidelines do not intend to address the circumstances under which a processing operation may fall within the exemptions from the consent requirement provided for by the ePD"* (§4).

Companies are surprised by the method chosen by the EDPB to focus on the sole cases of application of Article 5(3) whereas the same article explicitly provides two exceptions to its scope. Indeed, Article 5(3) also states that "*This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user*". AFEP member companies are therefore asking the EDPB to also recall and look into the assessment of these two exceptions in these guidelines and to provide some examples of situations where such exceptions would apply. **Indeed, the provisions of Article 5(3) need to be treated as a whole and not in part.**

As the ePD is more than 20 years old, these provisions also need to be adapted to the technological evolutions and the new products, services and uses they generated for the benefit of users.

With the EU Data strategy and the recent adoption of the Data Governance Act, Data Act and upcoming AI Act that require companies to process and share data more extensively, the EDPB should reconsider its interpretation of the ePD to promote EU innovation. Unfortunately, following the publication of the draft guidelines, some companies have already put several R&D projects on hold.

1.3. The notion of abuse

Companies also invite the EDPB to clarify what it means in §42 stating that "*once again, the abuse of those mechanisms (for example in the context of fingerprinting or the tracking of resource identifiers) can lead to the application of Article 5(3) ePD*". The notion of "*abuse*" used by the EDPB is indeed not defined and may be subject to many divergent interpretations and contribute to the fragmentation of the internal market. Moreover, the notion has not been developed before in these draft guidelines. AFEP member companies thus do not see what EDPB is referring to when writing "*once again*".

AFEP would also like to draw the attention of the EDPB to the following particular sections of its guidelines:

2. The notion of 'equipment' (section 2.3)

AFEP member companies note the analysis of the EDPB that application of Article 5(3) is not dependent on whether the electronic communication was initiated by the user or even on whether the user is aware of the said communication (§19).

They observe that this analysis is not directly foreseen in the ePD and would include in the scope of the directive all cases where the user is not involved in the communication from the terminal equipment, thus considerably broaden the scope of the ePD, and rendering the operational feasibility of some projects complex if not impossible.

3. The notion of 'electronic communications network' (section 2.4)

AFEP member companies observe a lack of development of the EDPB as regard the criteria of "*public availability*" of the communication services for Article 5(3) of the ePD to apply. Companies note that according to the EDPB granting access to a limited subset of the public does not make a network private, but they invite the EDPB to clarify under which conditions a communication network could be considered as a private network.

4. The notion of 'gaining access' (section 2.5)

AFEP member companies observe that the EDPB's interpretation of the notion of gaining access is particularly broad and raises serious concerns.

Companies share the view of the EDPB as regard the application of Article 5(3) when an accessing entity explicitly instructs the terminal equipment to send an information.

Nevertheless, AFEP member companies do not share the analysis of the EDPB when an entity uses protocols that imply the proactive sending of information by the terminal equipment which may be processed by the receiving entity. In this case, the external entity is a passive recipient of such information following an active action initiated by the terminal equipment. The words "*gaining of access*" clearly imply an active access to the user's terminal. If information is merely received by an entity (e.g. information that browsers automatically send when a website is called up), then the criterion relating to the "*gaining of access*" should not be considered as fulfilled. Otherwise, the letter and intent of the ePD would be twisted.

For clarity sake, the loading of any online resource would involve HTTP requests instructed by the terminal equipment, as the implementation of basic Internet protocols necessarily require an exchange of information. Thus, by adopting such an analysis, any Internet browsing by a user would thus trigger the application of Article 5(3) of the ePD for the display of any website page or email.

The broadening appreciation of the notion of gaining access would lead to the application of the ePD to cases far beyond the concept of access to information in the user's terminal: the current version of the guidelines would lead to the application of the ePD in situations where there is no access to information, as this information is merely transmitted *via* the HTTP protocol. This interpretation is not in line with the material scope of the ePD and the adoption of guidelines couldn't justify the broadening of the material scope of a Directive which should be undertaken by a legislative procedure.

Moreover, this approach seems disproportionate considering the objectives of the ePD to conciliate the freedom to conduct a business and the protection of the users 'privacy. On this last point in particular, AFEP member companies note that an extensive approach of Article 5(3) may also be detrimental to the user's experience who will be asked even more to give his/her consent and would participate to the so called "*consent fatigue*". In addition, by being requested to consent too extensively, users tend to consider consent as meaningless.

5. The notions of 'Stored Information' and 'Storage' (section 2.6)

The EDPB states 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*' (§36).

Yet, the ePD refers to "*the storing of information*, or *the gaining of access to information already stored*, *in the terminal equipment*". The use of the word "*already*" implies a notion of time. For this reason, it is questionable to consider that the legislator's intent was to cover information generated instantaneously (which is, by definition, not already stored in the terminal equipment) or stored "ephemerally".

Therefore, AFEP member companies encourage the EDPB to reconsider its draft guidelines on this aspect.

6. Use cases

As a preliminary remark, AFEP member companies observe that §43 in its current version would favour GAFAM in the use of information located inside the terminal that would be exempted from obtaining consent as long as the information does not leave the device. To the contrary, economic actors unable to develop local applications or web browsers and forced to develop their activities via Internet sites would see the application of the directive to their activities. This would reinforce existing dominant position and increase market distortions between economic operators in contradiction with the objectives of the DMA recently entered into force.

As regard URL and pixel tracking, AFEP member companies do not share the view of the EDPB that it constitutes storage on the communication network user's terminal equipment.

First, companies would like to emphasize that pixel tracking does not enable operators to track "*users' behaviour*" but solely to report information of received and opened emails. As such, these tools enable operators to analyse and improve their communication by limiting the sending of emails only to the individuals that have shown interest in these emails.

Moreover, from a technical point of view, pixel tracking does not involve accessing the user's terminal, nor the storage of information on said terminal. The displaying of a pixel in an e-mail causes the sending of a request to the remote server on which such pixel is located (as for any image), containing several pieces of technical information (date and time of the request, terminal characteristics). Such information is sent to the remote server using the HTTPS protocol. The processing of such information is caused by the opening of the e-mail on the terminal equipment by the user, but this information is not read on the user's terminal equipment (i.e. this information is in a server log).

In other words, when using pixel tracking, information is gathered solely on the basis of the message sent to the server when the HTTP request is executed, and not with the information stored or already existing in the user's terminal. Therefore, this technology cannot be included in the scope of Article 5(3) of the ePD.

In these circumstances, companies are surprised by §50 which states that tracking pixels and tracked URL constitute storage on the communication network user's terminal, without any demonstration.

From a usage point of view, considering that pixels in emails are tracking technologies, companies will no longer be able to ensure that emails containing information about a contract with individuals (e.g. modification of a password; price increase) have been read by them. It would deprive data controllers from a means of evidence which is absolutely necessary.

Should Article 5(3) apply to the pixel tracking, companies are wondering how to obtain consent for the "emailing" pixels. No technical solution is contemplated by the EDPB for the implementation of this consent.

Lastly, AFEP member companies note that even if Article 5(3) of the ePD does not apply to pixel tracking, companies remain fully subject to the provisions of the GDPR when there is a processing of a personal data. Thus, the use of these tools would remain within the oversight of data protection authorities.

ABOUT AFEP

Since 1982, AFEP brings together large companies operating in France. The Association, based in Paris and Brussels, aims to foster a business-friendly environment and to present the company members' vision to French public authorities, European institutions and international organisations. Restoring business competitiveness to achieve growth and sustainable employment in Europe and tackle the challenges of globalisation is AFEP's core priority. AFEP has over 110 members. More than 8 million people are employed by AFEP member companies and their annual combined turnover amounts to €2,600 billion. AFEP is involved in drafting cross-sectoral legislation, at French and European level, in the following areas: economy, taxation, company law and corporate governance, corporate finance and financial markets, competition, intellectual property, digital and consumer affairs, labour law and social protection, environment and energy, corporate social responsibility and trade.

Contacts:
Jocelyn Goubet – Director for Economic Law - j.goubet@afep.com
Alix Fontaine – European Affairs Deputy Director– a.fontaine@afep.com

Transparency Register identification number: 953933297-85