November 2024

Connect Europe's response to EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

Connect Europe welcomes the opportunity to comment on the draft Guidelines 01/2024. We appreciate the EDPB recognizes that *"the GDPR does not establish any hierarchy between the different legal bases laid down in Article 6(1)(f)"* and reaffirms the centrality of the accountability principle, which empowers controllers to determine the most suitable legal ground for a given data processing activity according to context.

The guidance underscores the robustness of the 'legitimate interests' legal basis and of the three-step assessment that underpins its use. If properly conducted, the balancing test required under Article 6(1)(f) results in processing operations that ensure a minimal interference with user privacy and fundamental rights after a rigorous evaluation of the stakes at play.

Consent fatigue is a widely recognised phenomenon in the online experience, largely due to misguided interpretations of the GDPR that seem to prioritise consent over other legal bases in all circumstances. As digitalisation becomes ever more pervasive, it is unrealistic to expect individuals to manage numerous consent requests daily from various controllers, often concerning complex activities that require significant attention to fully understand. This approach can lead to poor privacy outcomes.

The GDPR specifies six legal bases for data processing, each tailored to specific situations. A healthy balance among these bases is essential, as overreliance on consent can disrupt this equilibrium and place an undue burden on data subjects. Consequently, individuals may struggle to differentiate between consent requests that require their attention and those better handled by other legal bases. To prevent confusion and disengagement from privacy considerations, it is important not to overwhelm data subjects with excessive information.

Although the case-by-case evaluation of whether the legitimate interests legal basis can apply to any given processing undercuts legal certainty for data controllers, we are confident that thoroughly implemented processing based on legitimate interests can be in principle a sensible option for many purposes, including for commercial activities as suggested by the Court of Justice of the European Union (CJEU) in its recent judgment on Case C-621/22.

Against this backdrop, we regret that the flexible, risk-based, and accountability-based approach to personal data processing afforded by the GDPR is precluded to telecommunications providers that must handle traffic and location data in compliance with the ePrivacy Directive. Processing communication data may involve different levels of risks for the user, depending on the nature, purposes, and context of the processing operation at hand – similarly to other personal data in scope of the GDPR. Yet, telecom providers cannot decide on processing these data under the most suitable legal base according to the situation, and to safeguard data according to the risk for individuals. This very restrictive approach applied to a specific sector is no longer justified considering the fast-evolving nature of digital services and of today's challenges.

For instance, at a time when telecom providers are being urged to enhance their efforts to prevent financial fraud through text messaging and voice services, such as smishing and vishing, the ePrivacy Directive poses significant challenges. It substantially hinders telecom operators' ability to process metadata for legitimate purposes. Specifically, its provisions on fraud prevention are quite succinct and do not provide sufficient legal certainty.

Moreover, the implementation of the ePrivacy Directive varies significantly across Member States, meaning that the scope of what a telecom operator can do for fraud prevention using traffic data can differ greatly depending on national legislation. The ePrivacy Directive is clearly outdated, and its impact on the legal certainty of telecom operators regarding these activities is increasingly apparent.

It is also concerning that the flexibility offered by the GDPR is not reflected in the ePrivacy Directive, despite being accessible to other actors in the digital realm. To effectively prevent fraudulent activities, a harmonised and cross-border effort is often necessary.

We advocate for a modern data protection regulatory framework that ensures a level-playing field by applying the same rules for comparable services. This would enable the European telecom sector to fully reconcile their commercial interests, the protection of people's privacy and fundamental rights, and their broader societal role in today's digital ecosystem.