Contribution to the EDPB's guidelines on processing of personal data based on Article 6(1)(f) GDPR

November 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 1/2024 on processing of personal data based on Article 6(1)(f) of the GDPR.

Nevertheless, companies question the need to adopt new guidelines on this subject as the EDPB already adopted such guidelines in 2014. They moreover observe that the draft guidelines make numerous references to the Meta case[1], whereas most companies are not impacted by this ruling, and that the draft doesn't take into account new crucial issues like artificial intelligence, on which companies clearly need guidance.

In addition, AFEP member companies call the EDPB to adopt shorter guidelines that would provide **real support** for companies in implementing the GDPR, to facilitate their adoption and use by all companies, including SMEs. A harmonised analysis tool for the whole EU would be a useful aid for companies.

Companies are also surprised by the lack of consideration for safety and security issues in these draft guidelines. Video surveillance and access control are generally based on legitimate interest.

They also regret the lack of concrete examples in this project. These guidelines could contain a list of activities that would benefit from a presumption of being legitimate. **This point alone would bring clarity and encourage innovation around data in Europe**.

1. General comments

As a preliminary comment, AFEP member companies would like to remind the EDPB that they already draw the attention of the European Commission in November 2023 on the fact that personal data protection authorities (hereinafter "**DPAs**") and the EDPB are reluctant to implement the **risk-based approach on which the GDPR is based**. In this respect, they observe that DPAs and EDPB have a particularly restrictive approach, applying the GDPR to the letter and even adopting a position of maximum protection of personal data without consideration for the day-to-day business life and economic models of companies.

[1] CJUE, 4 July 2023, C-252/21.

It should be remembered that Recital 4 of the GDPR states that **the right to protection of personal data is not an absolute right**. It must be considered in relation to its function in society and balanced against other fundamental rights, in accordance with the **principle of proportionality**, which requires this protection to be weighed against all other fundamental rights, in particular freedom of enterprise. AFEP therefore considers that companies are faced with an **overly rigid and systematic interpretation of the texts**.

Thus, **AFEP member companies invite the EDPB to apply in these draft guidelines a reasonable risk-based approach** and avoid issuing guidelines that would end up applying a precautionary principle in practice that would annihilate innovation around data in Europe.

This reasonable risk-based approach is also necessary to align the GDPR with the evolution of the legal landscape in Europe. Since 2018, the EU has indeed recognised the economic value of data and the organised innovation around it by adopting several key legislations to enable the sharing of data and the development of data driven products and services (Data Governance Act, Data Act, Artificial Intelligence Act, etc.). **These have reshaped the central role that data plays in our societies and economies and the need for data to be shared and reused. The EDPB cannot ignore these important legislative developments**.

This reasonable risk-based approach is also made possible by the development of new technologies that hold great promises for the protection of personal data.

On this subject, AFEP member companies particularly encourage the EDPB and DPAs to take into account in their analysis the nature of the data to be processed. **Pseudonymised data convey less risk than directly identifying data**. The GDPR contains more than ten provisions recognising that pseudonymisation reduces risks for data subjects. The reliance on de-identification techniques such as pseudonymisation must be part of the balancing exercise to show that the data has a less personal character than directly identifiable data. The more sensitive the data, the greater the risk of a negative impact on the data subjects and conversely, **the less identifiable the data, the less the risk of a negative impact on the data subjects.**

On artificial intelligence, they note that the AI Act adopts a risk-based approach and focuses on the high-risk uses referred to in its Annex 3 – as they potentially affect the health, safety or fundamental rights of individuals.

It is therefore imperative that the approach of the data protection authorities does not only consider GDPR rules in isolation.

AFEP member companies also observe that the French AI commission in its report to the President of the Republic recommended returning to **the initial spirit of the GDPR** to reconcile personal data protection and innovation[2].

This issue has also been clearly identified in the recently issued DRAGHI report which states that "*while the ambitions of the EU's GDPR and AI Act are commendable, their complexity and risk of overlaps and inconsistencies can undermine developments in the field of AI by EU industry actors*". It also stresses **the risk of European companies being excluded from early AI innovations because of the uncertainty of regulatory frameworks as well as higher burdens for EU researchers and innovators to develop homegrown AI**.

Moreover, it is necessary to take into account the risk that many models will be excluded from the European market due to overly strict regulations or legal uncertainty generated by a conservative interpretation of these texts. This will put European companies at a competitive disadvantage with their non-EU competitors as they will not be able to use or rely on certain AI models to develop their own AI systems or applications. **Ultimately, this will be detrimental to European society as a whole**.

2. The legitimate nature of the interest pursued

AFEP member companies welcome the fact that the EDPB consider that there is no exhaustive list of interests that may be considered as being legitimate (see §16).

They consider indeed that a wide range of interests can be regarded as legitimate. This exercise is specific to the context of each assumption and depends on the circumstances of each use specific to each company. Thus solely a case-by-case analysis will allow the use of this legal basis.

Nevertheless, they would like to draw the attention of the EDPB to the fact that they process personal data to meet operational requirements or regulatory obligations.

These sectorial regulatory obligations are very high in Europe, and generally issued by EU law. These are implemented by companies as requested by law and not for their own convenience. Thus, the assumption that "*the interest of a controller to report fraudulent behaviour to competent law enforcement authorities may possibly outweigh the interests, rights and freedoms of the data subjects only if the controller processes data that is accurate and demonstrably relevant to assess whether a data subject is at risk of becoming the victim of fraud or is (un)reliable*" (see §105) seems disconnected from practical application of regulatory obligations and the goals of these regulations. AFEP thus invites the EDPB to exchange on this subject with enforcement authorities, namely in the financial sector.

[2] Commission de l'intelligence artificielle, mars 2024, IA : notre ambition pour la France, https://www.economie.gouv.fr/files/files/directions_services/cge/commission-IA.pdf.

On the first condition to be met in order to fulfil this presumption of legitimacy, companies are surprised by the reference to the lawfulness nature of the controller's interest. Indeed, according to article 5 of the Declaration of the Rights of Man and of the Citizen, "*anything that is not forbidden by law cannot be prevented*". Accordingly, the companies point out that this first criterion should instead be "*manifestly not unlawful under the law*" or "*not contrary to the law*" as initially stated by the CJEU[3]. **This point would encourage innovation.**

On the third condition to be met in order to fulfil this presumption of legitimacy, companies observe that research and development activities may be experimental - including hypothetical – namely in the field of AI systems, and that the interest would therefore not be real and present. **This criterion should be clarified so as not to exclude R&D work**. Otherwise, European companies could be excluded from research and development activities related to data.

On this point, AFEP member companies also note that reference to "*actual activities of the controller*" (see §19) may limit the use of this legal basis. Such wording seems to prohibit the development of new activities by a company, which is certainly not the objective pursued by the EDPB. **Such a general prohibition would inevitably hinder innovation and competition in the data sector by favouring existing players, and particularly hyperscalers, introducing barriers to market entry**.

3. The necessity of the processing to pursue the legitimate interest

AFEP member companies are surprised by the interpretation adopted by the EDPB on the necessity of the processing.

The EDPB seems indeed to establish an unfortunate hierarchy between the different legal basis, whereas article 6 of the GDPR doesn't establish such a hierarchy but to the contrary places them on an equal footing.

Companies note that the draft guidelines add stricter requirements on the use of legitimate interest compared to other legal bases when it states that a controller may rely on this legal basis "*only if it has also assessed and concluded that the envisaged processing **is strictly necessary for pursuing such a legitimate interest***" (see §13), whereas the GDPR only requires that the processing is necessary - not strictly necessary - for the purposes of the legitimate interests pursued by the controller or by a third party.

This constitutes a good illustration of the DPAs' and EDBP tendency to adopt a broad interpretation of legislation to the detriment of companies. Thus, **AFEP invites the EDPB to apply strictly the GDPR in these draft guidelines and not to extend it.**

[3] CJUE, 4 October 2024, C-621/22, §49.

4. The balancing exercise between the interests at stake

As a preliminary remark, companies would like to emphasize the fact that **the right to protection of personal data is not an absolute right**, as expressly stated by recital 4 of the GDPR. They believe that **this statement is the basis of the balancing exercise**.

AFEP member companies are surprised by the systemic use of the notion of "*opposing rights and interests*" (see §32). They do not share the view that the controllers' interests and the data subjects' interest are systematically opposed. To the contrary, companies believe that these interests are aligned very often as the processing of personal data is beneficial to the data subject.

The EDPB should not establish a hierarchy of legitimate interests. Above all, AFEP notes that a commercial interest may serve the interests of the customer, including an end consumer. Similarly, a commercial interest may also serve the public interest. Establishing a hierarchy of interests according to their commercial nature is not only intellectually unfounded but it is also biased and dangerous for innovation, which is often driven by private bodies. **This is also not the initial spirit of the GDPR**. The commercial interest, the user's interest, the public interest - including scientific research - and the general interest must not therefore be pitted against each other. In fact, it is imperative to be able to rely on the legal basis of legitimate interest so as not to restrict innovation in the field of data and namely AI.

Therefore, AFEP member companies share the view of the EDPB that "*the purpose of the balancing exercise is not to avoid any impact of the interests and rights of the data subjects altogether. Rather, its purpose is to avoid a disproportionate impact and to assess the weights of these aspects in relation to each other*" (see §33). Companies believe indeed that a mere impact on the interests and rights of the data subject should not prevent the data controller from relying on the legitimate interest legal basis.

In addition, AFEP member companies observe that the EDPB refers to "*more private*" data (see §40), without explanation, and without explicit reference to GDPR. Companies question this concept, which has no legal value. If EDPB wishes to make reference to more private data, it should conversely make reference to less private data. In any case, companies believe that this review remains a case-by-case analysis.

Finally, AFEP member companies observe that the EDPB require balancing tests to be made available to data subjects (see §68), which is not required by the GDPR. The EDPB believes that this "*transparency obligation*" stems from the accountability principle set out in Article 5(2) of the GDPR, whereas Article 13(1)(c) only requires controllers to provide "*the purposes of the processing for which the personal data are intended as well as the legal basis for the processing*", and not the balancing test by itself.

Once again, this constitutes a good illustration of the DPAs' and EDBP tendency to adopt a broad interpretation of legislation to the detriment of companies. Thus, **AFEP invites the EDPB to apply strictly the GDPR in these draft guidelines and not to extend it.**

5. The reasonable expectations of the data subject

To conduct the balancing exercise, the draft guidelines namely require the controller to identify and describe the "*reasonable expectations of the data subject*" (see §32).

As a preliminary remark, companies would like to draw the attention of the EDPB to the particularly delicate nature of such an exercise. Such a definition must not become an unreasonable administrative burden for controllers.

Therefore, it is key not to consider the expectation of each data subject separately, but to rely on the notion of an "*average*" consumer as §54 rightly provides which. This being an average, this means that some data subjects will clearly expect the processing activity, while others will not necessarily expect the processing. Moreover, this means that the "*professional position*" of the data subject may not be known and presumed by the controller. If this is the case, the EDPB needs to clarify this point. This however should not automatically mean that the interest of the data controller is not legitimate.

Likewise, clarification should be made to the notion of "*personal interests*" distinguished by the EDPB from financial or social interests (see §38).

In addition, the perceptions of the average data subject are not set in stone forever. Just like individuals have become more aware of their privacy rights because of the GDPR, they also have gained a better understanding on the functioning of Internet and how it is financed by advertising. The awareness of individuals that their data is being processed to enable advertisement is much higher today than it was when the GDPR entered into force. This has an effect on what is considered as a reasonable expectation.

On this point, companies finally note that "*possible broader emotional impacts*" (see §46) cannot be predicted by a controller as they strongly vary from one data subject to another. Therefore, they should not be taken into account in the balancing test.

6. Processing for direct marketing purposes

As stated above, AFEP member companies consider that a wide range of interests is capable of being regarded as legitimate. The interests analysis is specific to the context of each case and depends on the circumstances of each use specific to each company. Thus, solely a case-by-case analysis will allow the use of this legal basis.

Therefore, AFEP is surprised and doesn't share the assumption that "*the balancing test would hardly yield positive results for intrusive profiling and tracking practices [...] for example those that involve tracking individuals across multiple websites, location, devices or services*" (see §120). This general assumption has been adopted without a precise analysis of the circumstances at stake and doesn't take into account the possibility for the controller to rely on pseudonymised data that cannot be reidentified. This circumstance alone would change the result of the proportionality test.

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