Contribution to the Commission's questions to GDPR multistakeholder expert group for the Commission's 2024 report on the application of the GDPR

November 2023

1. General comments

a. What is your overall assessment (benefits/challenges, increase in trust and awareness, etc.) of the implementation of the GDPR since May 2018? Are there any priority issues that need to be addressed?

The GDPR has undoubtedly increased consumer confidence in the protection of their personal data and helped businesses to better organise their governance and processes for handling this data. As a result, companies have invested heavily in GDPR compliance.

Moreover, the GDPR has also become an international benchmark, encouraging other countries to adopt similar regulations.

However, AFEP companies deplore the fact that personal data protection authorities (hereinafter "DPAs") **are reluctant not to implement the risk-based approach on which the GDPR is based**. In this respect, they observe that DPAs 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**.

Nevertheless, the right to protection of personal data is not absolute: the GDPR recalls 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.**

For their part, individuals have a detailed knowledge of the extensive interpretation given by DPAs to the protection of their personal data. In this context, companies are seeing an increase in litigation, often brought by privacy actors on questions of principle without any material issue at stake or any infringement of the fundamental rights and freedoms of individuals.

This approach creates ongoing legal uncertainty for businesses, exacerbated by the lack of a harmonised approach at European level.
Such an approach also constitutes a disincentive for businesses to innovate and create value with data, particularly through artificial intelligence. While creating legal distortions that are hardly conducive to business, the approach adopted by the Italian DPA on ChatGPT is an illustration of Europe's appetite for new technologies, and jeopardises the attractiveness of the European economy.

Refocusing the assessment of DPAs on this risk-based approach is therefore a priority for AFEP in order to free companies from constraints that are disproportionate to the issues at stake, and to enable them to seize the opportunities offered by the development of new technologies based on the processing of personal and non-personal data.

2. Exercise of data subject rights

a. From the individuals' perspectives: please provide information on the exercise of the data subjects' rights listed below, including on possible challenges (e.g. delays in controllers/processors reply, clarity of information, procedures for exercise of rights, restrictions on the basis of legislative measures). etc.).

NA

From the controllers and processors' perspective: please provide information on compliance with the data subjects rights listed below, including on possible challenges (e.g. manifestly unfounded or excessive requests, difficulties in meeting deadlines, identification of data subjects, etc.).

As mentioned above, businesses are continually investing time and resources in developing and maintaining their compliance with the GDPR. However, they are facing difficulties in implementing the rights of data subjects.

For example, **companies do not have a DPA-validated solution for checking the identity of the person requesting a right and limiting the risk of unauthorised access to data.** The use of an identity card could be a solution, but the DPAs refuse this solution, deeming it too intrusive. Companies are therefore awaiting clarification on this point.

In addition, **companies are faced with a growing number of civil court proceedings resulting from the instrumentalisation of the rights of data subjects**, supported by law firms specialising in this area, **for questions of principle with no material issue at stake.**

Indeed, despite the measures taken by companies, and often for reasons of unintentional technical problems, non-compliance may persist despite the goodwill of the companies concerned.

In a digital economy, the possible consequences of non-compliance for the individuals concerned remain limited (receipt of a commercial e-mail or unwanted advertising). However, some courts deal with these cases without taking any account of the principle of proportionality, and the plaintiff can thus obtain substantial compensation without any objective justification.

This diverted use of the GDPR has already been identified in the Commission's previous report of June 2020 on the application of the GDPR, without the matter having been referred to the supervisory authorities.

- Information obligations, including the type and level of detail of the information to be provided (Articles 12 to 14)

NA

- Access to data (Article 15)

AFEP member companies note that the scope of the right of access is not clearly defined. Companies cannot assume by default that all data must be provided to the person making the request, particularly when the data has been pseudonymised and has very little to do with the rights and freedoms of the data subject.

In addition, some supervisory authorities appear to be extending the scope of access requests. For example, the French DPA states that when an employee makes a request for access to emails, the employer should provide "the content of the emails" and not the personal data contained in the email. This position goes beyond the provisions of the GDPR.

These requests entail a substantial workload for the companies, with a significant cost, while the gains for the applicants are particularly limited.

Certain specific requests raise other notable difficulties and demonstrate the instrumentalisation of the right of access.

Many of the people concerned (customers, employees, etc.) exercise their right of access not to check the accuracy of the data processed but to obtain documents which, for the most part, will be used to support a pre-litigation action. This is also apparent from the wording of access requests, which aim to obtain copies or duplicates of "documents" rather than copies of data.

AFEP companies have observed increasing requests from employees for access to their personal data on the basis of the GDPR. These requests relate in particular to emails, of which the employees are neither the author nor the recipient, but which mention their identity or elements likely to identify them. They are almost systematically part of pre-litigation cases with the employer. **Case law tends to adopt a broad if not incoherent view of employees' right of access, even though such requests must be assessed in the light of the principle of proportionality.** Companies are therefore faced with the difficulty of having to provide copies of emails containing purely internal information, which is necessary for their business and sometimes strategic for them. AFEP member companies therefore draw the Commission's attention to the fact that the rights and freedoms of third parties - both natural and legal persons - should also be taken into account when assessing such a request, including the business secrets and intellectual property of the companies concerned in a balanced approach to the essential principles of the GDPR, reconciling freedom and proportionality.

- Rectification (Article 16)

NA

- Erasure (Article 17)

AFEP member companies note that personal data for which the data subject exercises his/her right to erasure/right to object or withdraws consent could also be used to train an algorithmic/AI model. The limits of these rights should therefore be interpreted in the light of current technological developments and the low risk for data subjects, in order to encourage innovation.

- Data portability (Article 20)

Companies may receive mass requests for access and portability from private bodies (e.g. brokers) on the basis of a mandate signed electronically by the data subjects. These organisations use requests to exercise their rights to obtain data and documents which they then use in the course of their commercial activity.

Processing these requests via a proxy is complex and time-consuming. Above all, companies are unaware of the conditions under which the data collected in this way is re-used and stored by the authors of these requests.

- Right to object (Article 21)

NA

- Meaningful explanation and human intervention in automated decision making (Article 22)

NA

b. Do you avail of/are you aware of tools or user-friendly procedures to facilitate the exercise of data subject rights?

NA

c. Do you have experience in contacting representatives of controllers or processors not established in the EU?

NA

d. Are there any particular challenges in relation to the exercise of data subject rights by children?

NA

3. Application of the GDPR to SMEs

NA

4. Use of representative actions under Article 80 GDPR

NA

5. Experience with Data Protection Authorities

AFEP member companies would like the DPAs and the EDPB to be more transparent about their activities in order to encourage constructive dialogue with the business world.

a. What is your experience in obtaining advice from DPAs?

AFEP companies note that it is generally difficult to receive informal advice from DPAs on an individual basis. **They regret this lack of constructive dialogue prior to inspection investigations.**

For example, the French DPA generally asks companies to group their requests through their network head. This does not allow companies to ask DPAs specific questions relating to their business and projects. There have been some positive developments recently, notably the creation of legal assistance programs, but the number of projects selected is insufficient to meet the needs of the companies concerned.

AFEP member companies also note that it is difficult to obtain a written opinion from the French DPA. However, an oral opinion does not guarantee legal certainty for the companies concerned, especially if this opinion varies according to the people interviewed at the French DPA.

b. How are the guidelines adopted so far by the EDPB supporting the practical application of the GDPR?

AFEP member companies regret that there is no dialogue prior to the publication of a first draft of the guidelines with stakeholders, including companies, to allow the DPAs/EDPB to hear their point of view on the functioning of the market, practices and potential or real risks on individuals. Indeed, these guidelines are drafted behind closed doors, without any transparency on the possibility for any organisation (company or professional body) to be heard by the EDPB.

Furthermore, AFEP notes that there are very few changes between the first version published during the public consultation and the final version of the guidelines. They invite the authorities to conduct an educational exercise on the reasons why certain contributions received as part of the consultation process were not retained.

Regarding the approach adopted by the guidelines, AFEP member companies note that the EDPB favours an approach that protects individuals and does not take into account the fundamental rights of third parties or important public interests. They therefore invite the EDPB to return to the initial objective of the GDPR through a risk-based approach, taking into account the various interests involved.

With regard to the implementation of the EDPB guidelines, AFEP member companies observe that DPAs tend to consider that they are not bound by these guidelines. This situation increases legal uncertainty for companies and does not encourage them to rely on these guidelines.

Finally, AFEP warns about the lack of transparency on the progress of the EDPB work program. AFEP member companies are awaiting with interest the new version of the 2014 guidelines on pseudonymisation and anonymisation of data. They are surprised that it has taken so long to update the guidelines, even though this is a major issue for companies in the development of new technologies, particularly those related to AI. With regard to anonymisation in particular, these guidelines would provide greater legal certainty for companies by specifying the limits of the application of the GDPR.

c. Are DPAs following up on each complaint submitted and providing information on the progress of the case?

NA

d. Are you aware of guidelines issued by national DPAs supplementing or conflicting with EDPB guidelines?

AFEP member companies question the appropriateness of DPAs issuing guidelines at the national level, even though guidelines have already been adopted by the EDPB and the GDPR should, in principle, lead to complete harmonisation within the EU.

This proliferation of guidelines is a source of complexity and confusion for companies operating within the EU as a whole, which is very often the case in the digital and data processing sectors. The different national interpretations of the DPAs recreate barriers to the internal market and distortions of competition that the GDPR was initially intended to eliminate.

6. Experience with accountability and the risk based approach

a. What is your experience with the implementation of the principle of accountability?

The principle of accountability was introduced by the GDPR, which did away with prior administrative authorisations before any processing activity. AFEP member companies point out that this approach only works, however, if there is close cooperation between companies and DPAs to ensure companies' compliance on the basis of a risk-based approach adopted by the GDPR.

However, DPAs have adopted strict interpretations of the GDPR that are not based on a risk-based approach. As a result, AFEP member companies are questioning the need to conduct a risk analysis if the DPAs do not take this into account during their inspections.

In addition, companies expected the DPAs to be more fluid and flexible in managing compliance with the GDPR and to provide more support. Penalty decisions would therefore have been reserved for the most serious cases of non-compliance.

However, AFEP member companies note that exchanges are generally not possible with DPAs (see question 5.a above). Sharing points of view unfortunately only takes place in the context of contentious proceedings.

Under these conditions, **the principle of accountability has created new legal uncertainty for companies.** In contrast, the previous system of prior declaration or authorisation to DPAs offered companies a minimum of legal certainty.

This observation was already made by the Commission in the first report on the GDPR of June 2020 and has worsened over the last 3 years:

- The right to protection of personal data is now constructed as an absolute right, in disregard of the principle of proportionality ;
- Investigations and sanctions are also aimed at breaches with no real impact, and without taking into account all the circumstances involved;
- The efforts made by companies to reduce the risks associated with their data processing activities, for example by using pseudonymisation techniques, are not taken into account by the DPAs.

b. What is your experience with the scalability of obligations (e.g. appropriate technical and organisational measures to ensure the security of processing, Data Protection Impact Assessment for high risks, etc.)?

NA

7. Data protection officers

AFEP member companies are wondering about the obligations to appoint a Data Protection Officer within a group of companies, and the possibility of appointing just one for all the companies in the group.

8. Controller/processor relationship (Standard Contractual Clauses)

NA

9. International transfers

a. For controllers and processors: are you making use of the Standard Contractual Clauses for international transfers adopted by the Commission? If yes, what is your experience with using theses clauses?

AFEP member companies use the standard contractual clauses adopted by the Commission.

b. For controllers and processors: Are you using other tools for international data transfers? If yes, what is your experience with using theses clauses?

NA

c. Are there any countries, regional organisations, etc. with which the Commission should work in your view to concentrate safe data flows?

AFEP member companies would be interested in the Commission's work towards the adoption of adequacy decisions to facilitate data flows to the following countries: Tunisia, Morocco, Mauritius.

10. Have you experienced or observed any problems with the national legislation implementing the GDPR (e.g. divergences with the letter of the GDPR, additional conditions, gold plating, etc.)?

AFEP member companies have observed difficulties in coordinating the GDPR with other sector-specific rules, in particular with banking regulations relating to the fight against fraud and money laundering, and with regulations applicable to commercial telephone canvassing.

For example, Article 1 of Decree no. 2022-1313 of 13 October 2022 on the control of the days, times and frequency of unsolicited commercial telephone calls states that "*where the consumer refuses this canvassing during the conversation, the professional shall refrain from contacting him or attempting to contact him by telephone before the* ***expiry of a period of sixty completed calendar days from the date of this refusal***". This time-limited opposition to telephone canvassing contradicts the provisions of the GDPR, which provides for a right of opposition that is unlimited in time.

They also call for greater cooperation between sector authorities on these various issues.

11. Fragmentation/use of specification clauses

AFEP member companies note a high degree of fragmentation in the application of the GDPR between Member States. To their knowledge, the Italian and Spanish DPAs have not adopted as many guidelines as France, for example.

This fragmentation is particularly noticeable in the new technologies sector, notably in the assessment of the application of the GDPR to AI. The Spanish DPA has adopted a restrictive approach on this subject, and the Italian DPA has even temporarily banned the use of ChatGPT. For its part, the French DPA is currently conducting a public consultation on the creation of learning databases, in which it considers that these are compatible with the protection of personal data. However, the guidelines resulting from this consultation will have to be updated once the IA Act has been definitively adopted at the European level.

12. Codes of conduct, including as a tool for international transfers

a. Do you consider that adequate use is made of codes of conduct?

AFEP member companies regret that only two codes of conduct in the same cloud sector have been approved at the EU level, whereas the codes of conduct were intended to make it possible to specify the application of the GDPR in the various sectors of the economy by establishing an ongoing dialogue between companies and DPAs.

b. Have you encountered challenges in the development of codes of conduct, or in their approval process?

AFEP member companies have been waiting with interest for several months for a code of conduct on pseudonymisation currently being prepared by the Belgian DPA.

For its part, the French DPA has suspended discussions underway on the adoption of a code of conduct on advertising because of an investigation launched by the Belgian DPA. The suspension of this work in progress - not required by the GDPR - prevents companies from working with the regulator to clarify the application of the GDPR rules in their sector.

c. What supports would assist you in developing codes of conduct?

AFEP member companies are looking forward to greater involvement by DPAs in the drafting of codes of conduct. Joint work between DPAs and professional associations would be a useful way of advancing these projects.

The appointment of monitoring bodies that are more familiar with the specific characteristics and dynamics of companies than DPAs could contribute to a more pragmatic implementation of the GDPR.

13. Certification, including as a tool for international transfers

AFEP member companies are surprised that 5 years after the GDPR came into force, it is still not possible to obtain a single GDPR certification.

14. GDPR and innovation/new technologies

a. What is the overall impact of the GDPR on the approach to innovation and to new technologies?

AFEP member companies are concerned about the impact of the GDPR on innovation and new technologies.

In theory, the GDPR allows for a technology-neutral, pragmatic and risk-based approach, which provides the necessary space for innovation. However, this space is limited by the restrictive approach of DPAs in interpreting the rules.

As mentioned above, such an approach also constitutes a disincentive for companies to innovate and create value with data, in particular through artificial intelligence.

Lastly, AFEP notes that this negative impact on innovation had already been mentioned in the first report on the GDPR, without the subject having been raised by the supervisory authorities.

b. Please provide your views on the interaction between the GDPR and new initiatives under the Data Strategy (e.g. Data Act, Data Governance Act, European Health Data Space, etc.).

AFEP member companies note that there is a natural risk of friction between the GDPR, which is based on the principle of minimising and deleting data, and the European data strategy, which is based on the sharing and re-use of data.

Indeed, the DGA and the Data Act recognise the economic value of data and organise innovation around it. However, this vision is not shared by the DPAs.

Similarly, innovation in AI presupposes the availability of a large amount of data. As mentioned above, the Spanish and Italian DPAs have adopted a restrictive approach on this subject. While the French DPA has adopted a more open approach in its public consultation on the creation of learning databases, the guidelines resulting from this consultation will necessarily have to be updated after the final adoption of the IA Act at the European level.

Numerous European texts currently being drafted or recently adopted are being dealt with in silos without any overall vision by their initial drafters, creating confusion in their application, administrative burdens and legal risks that European players do not need.

Lastly, AFEP notes that this tension between AI and the GDPR was already mentioned in the first report on the GDPR, which already called for more exchanges between industry and data protection authorities on technological aspects.

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 117 members. More than 8 million people are employed by AFEP 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:
Emmanuelle Flament-Mascaret – Director for Economic Law – concurrence@afep.com
Jocelyn Goubet – Economic Law Direction - j.goubet@afep.com
Alix Fontaine – European Affairs Advisor – a.fontaine@afep.com

Transparency Register identification number: 953933297-85