FIVERS

Regulatory Update
Data protection, AI, IT and IP

No. 2 / 2025

DATA PROTECTION.

20 January 2024 – European Data Protection Board: the report on the CEF 2024 (Coordinated Enforcement Framework) on the state of implementation of the right of access by Data Controllers in the EU has been adopted.

---

17 January 2024 – European Data Protection Board: Guidelines 1/2025 on pseudonymisation published, in public consultation until 28 February 2025.

---

16 January 2024 – European Data Protection Board: a summary report on the decisions of the Data Protection Authorities on the right of access in the one-stop-shop (OSS) has been published.

---

16 January 2024 – European Data Protection Board: agenda and new measures.

---

14 January 2024 – CNIL: how to set up mobile apps in compliance with personal data protection regulations.

---

9 January 2024 – EU Court of Justice: interpretative clarifications on the notion of "excessive requests" pursuant to Article 57, paragraph 4, of the GDPR.

---

9 January 2024 – EU Court of Justice: the customer's gender identity is not a necessary piece of data for the purchase of a ticket.

ARTIFICIAL INTELLIGENCE.

7 January 2025 – The main trends and developments expected in 2025 for Artificial Intelligence.

DIGITAL MARKETPLACES

17 January 2025 – The DORA Regulation on Digital Operational Resilience is fully applicable.

---

16 January 2025 – The European e-Justice Strategy 2024-2028 is published in the Official Journal of the EU.

INFORMATION TECHNOLOGY

10 January 2025 – The new rules for carrying out civil and commercial mediation with telematic methods will come into force from 25 January 2025.

DATA PROTECTION

20 January 2024 – European Data Protection Board: the report on the CEF 2024 (Coordinated Enforcement Framework) on the state of implementation of the right of access by Data Controllers in the EU has been adopted.

The European Data Protection Board (EDPB) has adopted the **report on the implementation of the right of access by controllers,** which summarises the results of a series of coordinated national actions carried out in 2024 under the so-called CEF (*Coordinated Enforcement Framework*), a key action of the EDPB as part of its 2024-2027 strategy to streamline enforcement and cooperation between data protection authorities. During 2024, thirty data protection authorities across Europe launched coordinated investigations into controllers' compliance with the right of access, launching formal inquiries and requests for information from 1,185 controllers, consisting of small and medium-sized enterprises (SMEs), large companies active in different sectors and sectors, as well as various types of public bodies

The findings summarised in the report suggest that, while awareness of the importance of this right is widespread, there is a need for greater awareness of the *Guidelines 1/2022 on the right of access* that the EDPB has adopted. The EDPB has identified important areas of criticality regarding obstacles to the full implementation of the right of access: from the lack of documented internal procedures to manage access requests to inconsistent and excessive interpretations of the limits to the right of access; up to the obstacles often encountered by the data subjects due to formal requirements placed in the way by the holder (such as the request to provide an excessive number of identification documents). For each critical area, the report provides a list of non-binding recommendations to be taken into account by data controllers and data protection authorities.

Despite the existing challenges, two-thirds of the participating DPAs still assessed the level of compliance of the responding controllers with regard to the right of access from "medium" to "high". An important factor that impacted the level of compliance was the volume of access requests received by data controllers, as well as the size of the organization. More specifically, large controllers showed a higher level of compliance than small, low-resource organizations.

Positive results in terms of good practices have been observed in a number of EU states, such as the adoption of self-service systems that allow individuals to download their personal data themselves in just a few clicks and at any time.

The CEF 2025 (*Coordinated Enforcement Framework*) will cover the **implementation of the right to erasure**.

---

17 January 2024 – European Data Protection Board: Guidelines 1/2025 on pseudonymisation published, in public consultation until 28 February 2025.

The European Data Protection Board (EDPB) has published Guidelines 01/2025 on pseudonymisation for public consultation.

Reiterating the definition of "*pseudonymization*" contained in Article 4 of the GDPR, the EDPB recalled that pseudonymization can be partially or completely reversed, making the data referring to the natural person again identifiable (and therefore "personal"). This can be done by association, by linking the pseudonymized data to the original data or by tracing back to the original identification data through the use of additional information held by the controller for this purpose.

In addition, Guidelines 1/2025 highlight, among other things, that:

- Pseudonymization can help to meet data protection requirements, such as data protection by design and by default, security and additional measures for international transfers of personal data.
- In the case of disclosure to third parties, the controller must assess whether the risk reduction achieved by pseudonymisation for internal processing still exists;

- the data controller must inform data subjects about pseudonymisation processes involving their personal data and how such data can be used to identify them;
- Any breach of security that leads to some sort of reverse engineering of the data and re-identification constitutes a breach of personal data (*data breach*).

Regarding the technical measures and safeguards for pseudonymization, the EDPB pointed out that to implement pseudonymization, controllers should:

- determine the objectives they intend to achieve with this measure, to define the domain of pseudonymization;
- decide what data should be processed; and
- Determine certain information, such as which attributes will be pseudonymized, the pseudonymization method to be used, and who will execute and store it.

It will be possible to participate in the public consultation until 28 February 2025.

---

16 January 2024 – European Data Protection Board: a summary report on the decisions of the Data Protection Authorities on the right of access in the one-stop-shop (OSS) has been published.

On 16 January 2025, the European Data Protection Board (EDPB) published a summary report on the right of access under Article 15 of the General Data Protection Regulation (GDPR) as part of the decisions taken when applying the *one-stop-shop* (OSS) mechanism (according to which, if an organisation processes personal data in more than one EU Member State, it is not necessary for it to interact with all the data protection authorities of the countries in which it operates, identifying a single main supervisory authority - the Lead Supervisory Authority, LSA - which acts as a central point of contact).

Since the entry into force of the GDPR, data protection authorities have worked closely together to take an increasing number of one-stop-shop decisions on the right of access, as evidenced by the high volume of decisions available in the EDPB register on the subject. The report summarizing the *one-stop-shop* cases takes into account both EDPB Guidelines 01/2022 on the rights of data subjects - Right of access, and the relevant rulings of the EU Court of Justice. It also provides useful examples on the exercise of the right of access in various contexts (e.g.: in the case of fake profiles or accounts that pretend to be data subjects) and highlights the ways in which data protection authorities interpret the different components of the right of access in different cases.

---

16 January 2024 – European Data Protection Board: agenda and new measures.

The agenda of the next session of the European Data Protection Board, scheduled for 16 January, foreshadows interesting news. Among the topics under discussion for the forthcoming adoption of the relevant measures are: the guidelines on pseudonymization, the update of the operational guidelines for DPOs, the position paper on the interrelationship between competition law and data protection (I am also thinking of the recent rulings of the EU Court of Justice on the relationship between the relevant antitrust and data protection authorities and the perimeter of the power to intervene in the respective fields), until the results of the CEF 2024, as is known relating to the right of access.

---

14 January 2024 – CNIL: how to set up mobile apps in compliance with personal data protection regulations.

The French Data Protection Authority (CNIL) has announced the publication of privacy recommendations for mobile apps. The recommendations highlight how access permissions can be implemented in the context of mobile apps.

The recommendations emphasize that technical authorizations must be distinguished from requests for consent. Users must be able to understand, by accepting or rejecting permissions, what data they are

sharing with apps. For example, location access is exempt from consent for the very operation of a navigation app, since the data is necessary for a service. Moreover, even when consent is required, a simple request for permission does not always imply free, specific, informed and unambiguous consent under the GDPR.

The recommendations also include *best practices* for operating system vendors in implementing a permissions system, which should allow operating system vendors to choose:

- the degree of precision of the data provided depending on the purpose pursued (e.g. more or less precise location);
- the material scope of the permission (e.g. access to the selected photos rather than to the overall media gallery); and
- the duration during which the authorization is granted (for example, one-time activation of the authorization or for a predetermined duration).

Finally, data controllers should determine whether permission-related processing involves read/write operations that require user consent. In this specific case, the implementation of a consent management platform may be required for the addition of a technical authorization request.

---

9 January 2024 – EU Court of Justice: interpretative clarifications on the notion of "excessive requests" pursuant to Article 57, paragraph 4, of the GDPR.

Article 57, paragraph 4, of Regulation 679/2016 ("GDPR") provides that the supervisory authority may charge a reasonable fee based on administrative costs or refuse to comply with the requests of the subjects who turn to it (including when lodging a complaint or requests for access) if the requests are manifestly unfounded or excessive, in particular for the repetitive nature, it is for the supervisory authority to demonstrate the manifestly unfounded or excessive nature of the request.

Max Schrems, a well-known Austrian business, had submitted 77 complaints to the Austrian privacy authority (DSB) - in a period of about 20 months - regarding the refusal of a well-known social network to verify his requests for access. Complaints rejected by the Austrian privacy authority as they were considered excessive for their number.

The Court of Justice of the European Union (CJEU) ruled on Case C-416/23, stating that "excessive" access requests under the GDPR cannot be considered as such only because of their number. The CJEU first clarified that, pursuant to Article 57(4) of the GDPR, the term "request" also includes complaints pursuant to Art. 77 of the GDPR. In addition, requests cannot be classified as 'excessive' within the meaning of Article 57(4) of the GDPR solely because of their number over a given period, since the exercise of the option provided for in that provision is subject to the demonstration by the supervisory authority of the existence of abusive intent on the part of the person who made those requests. Finally, when faced with excessive requests, a supervisory authority may choose, by reasoned decision, between charging a reasonable fee based on administrative costs or refusing to comply with the request, taking into account all relevant circumstances and ensuring that the preferred option is appropriate, necessary and proportionate.

---

9 January 2024 – EU Court of Justice: the customer's gender identity is not a necessary piece of data for the purchase of a ticket.

The Mousse association challenged before the French authority for the protection of personal data (the CNIL) the practice of the French railway undertaking SNCF Connect, which systematically obliges its customers to indicate their title ('Sir' or 'Madam') when purchasing tickets online. That association considers that that obligation infringes the General Data Protection Regulation (GDPR), in particular from the point of view of the principle of data minimisation, since the indication of the title, which corresponds to a gender identity, does not appear to be necessary for the purchase of a rail transport ticket. In 2021, the CNIL decided to reject that complaint, taking the view that the practice did not constitute a violation of the GDPR.

Disapproving of that decision, Mousse brought an action before the Conseil d'État (Council of State, France) for annulment. The Conseil d'État (Council of State) asks the Court of Justice, inter alia, whether

the collection of data relating to the title of customers, limited to the terms 'Sir' and 'Madam', may be classified as lawful and compliant, inter alia, with the principle of data minimisation, where that collection is intended to enable personalised commercial communication to those customers, in accordance with the generally accepted customs in this area.

The Court recalls that, in accordance with the principle of data minimisation, which is an expression of the principle of proportionality, the data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In addition, the Court recalls that the GDPR provides for an exhaustive and exhaustive list of cases in which the processing of personal data may be considered lawful: this is the case, in particular, where (i) it is necessary for the performance of a contract to which the data subject is a party, or (ii) it is necessary for the pursuit of the legitimate interest of the controller or of a third party.

As regards the first of those two justifications, the Court recalls that, in order for data processing to be regarded as necessary for the performance of a contract, that processing must be objectively indispensable in order to enable the proper performance of that contract. In that context, the Court considers that the personalisation of commercial communication based on a presumed gender identity on the basis of the customer's title does not appear to be objectively indispensable in order to enable a rail transport contract to be properly performed. The railway undertaking could opt for communication based on generic politeness formulas, inclusive and unrelated to the presumed gender identity of customers, which would be a viable and less intrusive solution.

As regards the second justification, the Court, while recalling its settled case-law on the subject, states that the processing of data relating to the title of the customers of a transport company, with the aim of personalising commercial communication based on their gender identity, cannot be considered necessary (i) where the legitimate interest pursued was not indicated to those customers at the time of collection of those data; (ii) if the processing is not carried out within the limits strictly necessary for the realization of such legitimate interest; or (iii) where, in the light of all the relevant circumstances, the fundamental rights and freedoms of those customers may override that legitimate interest, in particular because of a risk of discrimination on grounds of gender identity.

ARTIFICIAL INTELLIGENCE.

7 January 2025 – The main trends and developments expected in 2025 for Artificial Intelligence.

2025 is the year of the first practical application of some parts of the EU Regulation 2024/1689 on Artificial Intelligence (AI Act). For example, as of February 2, 2025, AI literacy requirements for staff will be applicable and the official definitions of Article 3 of the AI Act may be used in contracts.

But 2025 will also be the year in which even more substantial developments in AI capacity are expected. Think of the so-called "*Artificial Intelligence Agent*", real AI agents capable of acting autonomously, making autonomous decisions and optimizing processes. For example: virtual assistants can not only answer questions, but manage entire marketing campaigns, personalize the user experience in real time, and automate complex tasks. This will lead to a new era of work automation and extreme customization.

2025 will bring new cybersecurity challenges, and companies will need to strengthen their security measures to cope with entirely new threats, such as *prompt injection* attacks, in which malicious inputs are disguised as seemingly legitimate messages and introduced into generative AI systems. Advances in *quantum computing* will also challenge traditional methods of cryptography.

Finally, recently published research by Cisco, Gartner and Capgemini Research Institute identifies the following 10 trends that will characterize AI in 2025:

#1: Agency AI reshapes the future of work automation
#2: AI-driven robotics blurs the lines between man and machine
#3: Space for governance platforms for AI
#4: New tools to counter misinformation and protect brand integrity

#5: Post-quantum cryptography to prepare for future threats
#6: The Era of Invisible Ambient Intelligence
#7: Energy-efficient computational computing reduces IT's carbon footprint
#8: Space computing spreads in the enterprise
#9: Multi-functional robots improve human-machine collaboration
#10: Hybrid computing to overcome the limitations of current analytical models.

DIGITAL MARKETS

17 January 2025 – The DORA Regulation on Digital Operational Resilience is fully applicable.

From 17 January 2025, after entering into force on 16 January 2023, Regulation 2022/2554 - *Digital Operational Resilience Act* (DORA) is fully applicable to financial entities within the EU.

The DORA Regulation prescribes uniform requirements on the security of network and information systems to support the commercial activities of financial entities, including credit institutions, payment institutions, investment firms, liquidity providers. Third-party ICT service providers are also indirectly affected by its application.

The DORA Regulation has introduced several technical, organisational and documentary requirements for the management of digital operational resilience, including:

- ICT risk management, including risk assessments, policies and threat monitoring;
incident detection and reporting, including (1) identifying major ICT-related incidents and notifying competent authorities of significant cyber threats on a voluntary basis; (2) the reporting to the competent authorities of serious operational or security incidents related to payments by certain financial entities;
- complete a series of assessments, tests, methodologies and practices to identify weaknesses, deficiencies and gaps in digital operational resilience;
- share information and intelligence in relation to cyber threats and vulnerabilities; and
- the implementation of measures for the proper management of ICT risks arising from third parties, such as the performance of a preliminary assessment, the implementation of an ICT risk strategy by third parties and a register of information on contractual arrangements, as well as the inclusion of key contractual provisions in contractual arrangements.

---

16 January 2025 – EU Council: the European e-Justice Strategy 2024-2028 has been published in the EU Journal.

Communication C/2025/437 of the EU Council on the European e-Justice Strategy 2024-2028 has been published in the Official Journal of the EU.

It applies to all Member States and should serve as a reference for all EU actors involved in the digital transformation process in the justice sector.

The strategy aims to identify the strategic and operational objectives and principles that should be respected in carrying out this digital transformation process, putting in place organisational and methodological measures, identifying key factors to facilitate and promote digitalisation, as well as promoting mechanisms to facilitate the coordination and follow-up of progress made in e-justice initiatives.

In particular, the communication lays down both *substantive* and *operational principles*.

The former include respect for fundamental principles and rights; access to justice; the centrality of people; bridging the digital divide; strengthening digital protections for users; make the system sustainable.

Among the operating principles , the Communication mentions the 'once-only' principle; the so-called '*digital by default*' principle; interoperability and cybersecurity; dynamic justice; data-driven justice; open source.

The general objective of e-Justice must always be to improve the provision of justice services to the public in order to facilitate the enjoyment of the right to effective judicial protection.

With this in mind, the following strategic objectives should be pursued:

- improving access to digital justice;
- strengthening digital judicial cooperation;
- making digital justice more efficient;
- promoting innovative digital justice.

INFORMATION TECHNOLOGY

10 January 2025 – The new rules for carrying out civil and commercial mediation with telematic methods will come into force from 25 January 2025.

With the publication in the Official Gazette of 10 January 2025 no. 7 of Legislative Decree 216/2024 - corrective to the Cartabia and in force since 25 January 2025 - important innovations and updates have been introduced to the civil and commercial mediation system, with the aim of making mediation more efficient and modern.

The new Article *8-bis* of Legislative Decree 28/2010 – entitled *Mediation in telematic mode* – provides for the digitization of the mediation process, with the consent of the parties. In this case, the documents of the proceedings are drawn up by the mediator and signed with digital signatures. At the end of the procedure, the mediator prepares an electronic document containing the minutes and any agreement for the affixing of the digital signature by the subjects who are required to do so (the document must be immediately signed and returned to the mediator). The mediator, upon receipt of the document and having verified the affixing of the signatures, validity, and integrity of the signatures, shall affix his signature and arrange for it to be deposited with the secretariat of the body, which shall send it to the parties and their lawyers, if appointed.

The new Article *8-ter* of Legislative Decree 28/2010 – entitled *Mediation meetings with remote audiovisual mode* – provides that each party can always ask the head of the mediation body to participate in meetings with remote audiovisual connection, provided that this ensures the contextual, effective and reciprocal audibility and visibility of the connected persons.
