FIVERS

Regulatory update
Data protection, AI, IT and IP

n. 6 / 2024

DATA PROTECTION

17 July 2024 – The European Data Protection Board – EDPB adopted two Frequently Asked Questions (FAQ) documents concerning the EU-U.S. Data Privacy Framework (DPF), aimed at providing more clarification on the functioning of the DPF.

---

17 July 2024 – The EDPB approves the *European Data Protection Seal* for the certification of processing activities by data controllers.

ARTIFICIAL INTELLIGENCE.

12 July 2024 - EU Regulation 2024/1689 (Artificial Intelligence Act) published in the Official Gazette.

17July 2024 – The European Data Protection Board - EDPB adopts a statement on Data protection Authorities' role in AI Act framework.

DIGITAL MARKETS.

17 July 2024 – EU General Court dismisses the action brought by Bytedance (TikTok) against the decision of the EU Commission designating it as a gatekeeper under the Digital Markets Act.

---

12 July 2024 – EU Commission sends preliminary findings to X for breach of the Digital Services Act.

INFORMATION TECHNOLOGY

12 July 2024 - Court of Cassation: in the case of an erroneous wire transfer, the bank is liable if it does not check the correspondence between IBAN and payee and cannot invoke privacy to refuse to provide the payee's personal data.

---

9 July 2024 - Court of Cassation: an appeal against dismissal transmitted by sending a certified electronic email (PEC) with a word file attached is valid.

---

8 July 2024 - Council of State: unlawful exclusion of a competitor from a tender for having sent its technical offer via the We Transfer service.

DATA PROTECTION

17 July 2024 – The European Data Protection Board – EDPB adopted two Frequently Asked Questions (FAQ) documents concerning the EU-U.S. Data Privacy Framework (DPF), aimed at providing more clarification on the functioning of the DPF.

The **FAQ for individuals** provides information on the functioning of the DPF: how to benefit from it, how to lodge a complaint and how this complaint will be handled.

Likewise, the **FAQ for businesses** explains which U.S. companies are eligible to join the DPF: what to do before transferring personal data to a company in the U.S. which is DPF-certified, and where to find further guidance.

---

17 July 2024 – The EDPB approves the *European Data Protection Seal* for the certification of processing activities by data controllers.

The EDPB adopted an opinion approving the EuroPriSe Criteria Catalogue for the certification of processing activities by data controllers resulting in a *European Data Protection Seal*.

In September 2022, the EDPB had adopted an **opinion on the EuroPriSe certification criteria**, enabling their recognition in Germany as certification criteria for processing operations by processors.

Following an update of the scheme, this new opinion approves the criteria as being applicable in the whole EU/EEA, and as a European Data Protection Seal.

GDPR certification contributes to the demonstration of compliance efforts and to increased transparency and trust. It allows for better assessment of the degree of protection offered by products, services, processes or systems used by organisations that process personal data.

The EuroPrise European Data Protection Seal will be added to the **register of certification mechanisms and data protection seals** in accordance with Article 42(8) GDPR and will be made available on the EDPB website.

ARTIFICIAL INTELLIGENCE.

12 July 2024 - EU Regulation 2024/1689 (Artificial Intelligence Act) published in the Official Gazette.

The Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) has been published in the Official Journal of the European Union on 12nd July 2024.

The Regulation 2024/1689 is the world's first comprehensive law on AI and aims to address risks to health, safety, and fundamental rights. In addition, it protects democracy, the rule of law and the environment.

The Regulation 2024/1689 shall enter into force on 1st August 2024, but it will only be **applicable from 2nd August 2026**. However, some rules will apply after 6 or 12 months.

The following will be **applicable from 2nd February 2025**:

(a) Articles 1 to 4, relating to the subject matter, scope, definitions (supply contracts may therefore use technical and legal definitions of the AI Act) and AI literacy obligations (obligation for suppliers

and developers to have trained and competent personnel, who may find specific entry into contracts with suppliers).
(b) Article 5 on prohibited AI practices (particular attention will have to be paid – for example – to advanced profiling using biometrics, especially in the workplace, to check the applicability of the ban).

After 12 months (**from 2nd August 2025**) the following will apply:

(a) the rules on the penalty system (with penalties of up to €35 million or 7% of annual global turnover; the penalty for providers of AI models for general purposes – up to €15 million or up to 3% of turnover – will apply after 24 months);
(b) the rules on General Purposes AI models (GPAI) (from which relevant compliance and contractual issues arise, considering that companies already use on a daily basis solutions – such as Chat-GPT and generative AI – integrated into devices/services);
(c) the rules on notified bodies and on the related notification procedures;
(d) Article 78 *("Confidentiality*");
(e) the rules establishing the EU database on high-risk AI systems.

Finally, the applicability of the rules on "high-risk" AI systems, as well as the related obligations, is postponed to **2nd August 2027**.

The Regulation 2024/1689 shall apply to public and private entities, inside and outside the EU, provided that an AI system is placed on the EU market or that its use affects persons located in the EU.

The rules will bind both providers/developers of AI systems (e.g. a developer of a CV screening tool) and professional end-users (called "deployers") of high-risk AI systems (e.g. a company that purchases the aforementioned screening tool).

The Regulation 2024/1689 will also apply to the entire commercial chain (importers, distributors, manufacturers of products who place an AI system on the market or put into service together with their product and with their name or brand, etc.): importers of AI systems in the EU will have to ensure, for example, that the non-EU supplier has already performed the appropriate conformity assessment procedure and that the AI system bears a European conformity (EC) and is accompanied by the required documentation and instructions for use.

There are also specific obligations for providers of general-purpose AI models (GPAIs) including large generative AI models (LLM systems – Large Language Models, such as Chat-GPT, Copilot, Gemini, etc.).

Providers of free and open-source models are exempt from most of these obligations. However, this exemption does not cover obligations applicable to providers of GPAI general purpose AI models that involve systemic risks.

Regulation 2024/1689 shall not apply to research, development and prototyping activities prior to placing on the market and to AI systems developed for military, defence or national security purposes, regardless of the type of entity carrying out such activities.

17July 2024 – The European Data Protection Board - EDPB adopts a statement on Data protection Authorities' role in AI Act framework.

During its latest plenary, the European Data Protection Board (EDPB) adopted a **statement on the Data Protection Authorities' (DPAs) role in the Artificial Intelligence Act (AI Act) framework**.

According to the EDPB, DPAs already have experience and expertise when dealing with the impact of AI on fundamental rights, in particular the right to protection of personal data, and should therefore be designated as Market Surveillance Authorities (MSAs) in a number of cases. This would ensure better

coordination among different regulatory authorities, enhance legal certainty for all stakeholders and strengthen the supervision and enforcement of both the AI Act and EU data protection law.
According to the AI Act, Members States shall appoint MSAs at national level before 2 August 2025, for the purpose of supervising the application and implementation of the AI Act.
In its statement, the EDPB recommends that:

- As already indicated in the AI Act, DPAs should be designated as MSAs for high-risk AI systems used for law enforcement, border management, administration of justice and democratic processes;
- Member States should consider appointing DPAs as MSAs also for other high-risk AI systems, taking account of the views of the national DPA, particularly where those high-risk AI systems are in sectors likely to impact natural persons rights and freedoms with regard to the processing of personal data;
- DPAs, where appointed as MSAs, should be designated as the single points of contact for the public and counterparts at Member State and EU levels;
- Clear procedures should be established for cooperation between MSAs and the other regulatory authorities which are tasked with the supervision of AI systems, including DPAs. In addition, appropriate cooperation should be established between the EU AI Office and the DPAs/EDPB.

DIGITAL MARKETS.

17 July 2024 – EU General Court dismisses the action brought by Bytedance (TikTok) against the decision of the EU Commission designating it as a gatekeeper under the Digital Markets Act.

Bytedance Ltd is a company which, via its subsidiaries, provides the online social networking platform TikTok. By decision of 5 September 2023, the EU Commission designated Bytedance as a gatekeeper pursuant to the Digital Markets Act (DMA). In November 2023, Bytedance brought an action for annulment of that decision.

By its judgment, delivered eight months after the action was brought, the Court dismisses Bytedance's action. The Court first recalled the legislative history and content of the DMA. It notably emphasised that the EU legislature decided to adopt the DMA in order, inter alia, to contribute to the proper functioning of the internal market by laying down rules to ensure the contestability and fairness of markets in the digital sector in general, and for business users and end users of core platform services provided by gatekeepers in particular.

The Court next found that the EU Commission was fully entitled to consider that Bytedance was a gatekeeper. In that connection, it observed that it was common ground that Bytedance met the quantitative thresholds laid down in the DMA, regarding, inter alia, its global market value, the number of TikTok users within the European Union and the number of years during which that threshold relating to user numbers had been met, so that it could be presumed that it was a gatekeeper. It went on to consider that the arguments submitted by Bytedance were not sufficiently substantiated so as manifestly to call into question the presumption that Bytedance had a significant impact on the internal market, that TikTok was an important gateway allowing business users to reach their end users and that Bytedance enjoyed an entrenched and durable position.

---

12 July 2024 – EU Commission sends preliminary findings to X for breach of the Digital Services Act .

The EU Commission has informed X of its preliminary view that it is in breach of the Digital Services Act (DSA) in areas linked to dark patterns, advertising transparency and data access for researchers.

Transparency and accountability in relation to content moderation and advertising are at the heart of the DSA. Based on an in-depth investigation that included, among others, the analysis of internal company

documents, interviews with experts, as well as cooperation with national Digital Services Coordinators, the Commission has issued preliminary findings of non-compliance on three grievances:

- First, X designs and operates its interface for the "verified accounts" with the "Blue checkmark" in a way that does not correspond to industry practice and **deceives users. Since anyone can subscribe to obtain such a "verified" status**, it negatively affects users' ability to make free and informed decisions about the authenticity of the accounts and the content they interact with. There is evidence of motivated malicious actors abusing the "verified account" to deceive users.
- Second, X does not comply with the **required transparency on advertising**, as it does not provide a searchable and reliable advertisement repository, but instead put in place design features and access barriers that make the repository unfit for its transparency purpose towards users. In particular, the design does not allow for the required supervision and research into emerging risks brought about by the distribution of advertising online.
- Third, X fails to **provide access to its public data to researchers** in line with the conditions set out in the DSA. In particular, X prohibits eligible researchers from **independently accessing** its public data, such as by scraping, as stated in its terms of service. In addition, X's process to **grant eligible researchers access to its application programming interface (API)** appears to dissuade researchers from carrying out their research projects or leave them with no other choice than to pay disproportionally high fees.

By sending preliminary findings, the EU Commission informs X of its preliminary view that it is in breach of the DSA. This is without prejudice to the outcome of the investigation as X now has the possibility to exercise its rights of defence by examining the documents in the Commission's investigation file and by replying in writing to the Commission's preliminary findings. In parallel, the European Board for Digital Services will be consulted.

If the Commission's preliminary views were to be ultimately confirmed, the Commission would adopt a non-compliance decision finding that X is in breach of Articles 25, 39 and 40(12) of the DSA. Such a decision could entail fines of up to 6% of the total worldwide annual turnover of the provider, and order the provider to take measures to address the breach. A non-compliance decision may also trigger an enhanced supervision period to ensure compliance with the measures the provider intends to take to remedy the breach. The Commission can also impose periodic penalty payments to compel a platform to comply.

INFORMATION TECHNOLOGY

12 July 2024 - Court of Cassation: in the case of an erroneous wire transfer, the bank is liable if it does not check the correspondence between IBAN and payee and cannot invoke privacy to refuse to provide the payee's personal data.

A bank, in executing a wire transfer order of one of its customers, had failed to notice the mismatch between the IBAN indicated in the order and the name of the payee indicated. Asked by the client to provide the data of the recipient of the sums in error, the bank had refused, claiming that it could not accept to the client's request because of the data protection laws.

The First Civil Section of the Supreme Court, on the contrary, in Order No. 17415/2024, pronounced the following principle of law: '*on the subject of a bank's liability for transactions effected by electronic means, when the beneficiary, named by name, of a payment to be effected by wire transfer is without a credit account with the intermediary bank, so that the specific rules under Article 24 of Legislative Decree No. 11 of 2010 cannot be used either, the rules of the law of the Italian Republic on the protection of personal data shall apply. 11 of 2010, the rules of ordinary law apply, so that the intermediary bank itself, liable, under the theory of 'qualified social contact', towards the beneficiary who has remained unsatisfied because of the indication, which has proved to be inaccurate, of its IBAN, bears the burden of proving that it has carried out the payment transaction requested by the solvency obligor, adopting all the necessary precautions in order to avoid the risk of an erroneous identification of that beneficiary, or, at the very least, of having endeavoured to enable the latter to identify the person who actually received the payment*

intended, on the contrary, for the former, also by communicating to him, where necessary, the relevant personal data'.

---

9 July 2024 - Court of Cassation: an appeal against dismissal transmitted by sending a certified electronic email (PEC) with a word file attached is valid.

The Court of Cassation specifies that the requirement of challenging dismissal in writing, in the absence of the provision of specific modalities, must be considered fulfilled also by sending a PEC with a word file attached.

In Order No. 18529 of 8 July 2024, the Labour Section set out the following principle of law:

"*Pursuant to Article 6 of Law no. 604/66, the requirement to challenge the dismissal in writing must be considered fulfilled, in the absence of the provision of specific modalities, by any method involving the transmission to the addressee of any written document whose content is capable of communicating the employee's intention to challenge the dismissal and which can be referred to him/her with certainty, therefore also by sending a PEC with a word file attached, since it is not necessary to send a computer copy of an analogue document pursuant to Article 22 of legislative decree no. 82 of 2005".*

---

8 July 2024 - Council of State: unlawful exclusion of a competitor from a tender for having sent its technical offer via the We Transfer service.

The Council of State, in its ruling no. 5789/2024, ruled on the appeal brought by a company concerning its exclusion from a tender for the award of a contract for the construction of university lecture halls.

The Regional Administrative Court of Calabria had rejected the appeal, claiming that the appellant had not complied with the instructions for the submission of offers, and in fact - due to the impossibility of uploading the entire technical offer on the tender platform due to capacity constraints - the company had transmitted the technical offer via *We Transfer.*

However, the Council of State upheld the appeal, clarifying that the sending of the technical bid via *WeTransfer* does not legitimise the exclusion of the bidder for the breach of the principle of secrecy of bids. This is especially so when overly rigid electronic platforms are chosen that make it difficult to submit bids, as in the case examined by the Council of State.
