FIVERS

Regulatory update
Data protection, AI, IT and IP

n. 11 / 2024

DATA PROTECTION

26 September 2024 - Supreme Court of Cassation: filing an audio file within a judicial proceedings do not infringe any privacy rights.

---

27 September 2024 – EU Court of Justice: personal data protection, the supervisory authority is not obliged to exercise a corrective power in all cases of breach and, in particular, to impose a fine.

ARTIFICIAL INTELLIGENCE.

25 September 2024 – EU Commission: over a hundred companies sign EU AI Pact pledges to drive trustworthy and safe AI development.

---

25 September 2024 – EU Commission: Code of practice for general-purpose artificial intelligence shall be adopted within April 2025.

---

24 September 2024 – Europol published a report on the benefits and challenges of artificial intelligence (AI) for law enforcement.

DIGITAL MARKETS

25 September 2024 - G7 Cyber Expert Group Recommends Action to Combat Financial Sector Risks from Quantum Computing.

INFORMATION TECHNOLOGY

25 September 2024 – Legislative Decree No. 134 of 4 September 2024 on 'Implementation of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical players' published in the Official Gazette.

DATA PROTECTION

26 September 2024 - Supreme Court of Cassation: filing an audio file within a judicial proceedings do not infringe any privacy rights.

Defending oneself in court, especially when the dispute relates to personal rights closely linked to human dignity - and thus the rights of workers, according to Article 36 of the Italian Constitution. - is a fundamental right and, in the relationship between employer and employee, legitimate expectations are created and, among these, that of mutual loyalty and respect for the employee's rights; Articles 17 and 21 of the GDPR make it clear that, in balancing the interests at stake, the right to defend oneself in court may be deemed to prevail over the rights of the data subject to the processing of personal data; in particular, Art. In particular, Article 17(3)(e) of the GDPR provides that paragraphs 1 and 2 (right to erasure) do not apply to the extent that processing is necessary for the establishment, exercise or defence of legal claims, and Article 21 (right to object) allows the data controller to demonstrate 'the existence of compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims'.

This is how the Civil Cassation expressed itself in Ordinance No. 24797/2024, in which it re-acknowledged the right of some workers to produce in court an audio file containing the recording of a conversation (among other things, dating back years) with the managers and legal representatives of the company that had appealed to the Guarantor (rejected) for violation of the principle of lawfulness and fairness in processing. The Court of Venice had annulled the decision of the Privacy Guarantor, while the Court of Cassation ordered the annulment with reference on the basis of the above considerations.

---

27 September 2024 – EU Court of Justice: personal data protection, the supervisory authority is not obliged to exercise a corrective power in all cases of breach and, in particular, to impose a fine.

In Germany, a savings bank found that one of its employees had consulted a customer's personal data on several occasions without being authorised to do so.

The savings bank did not inform the customer of this, as its data protection officer had taken the view that there was no high risk for him. The employee had confirmed in writing that she had neither copied nor retained the data, that she had not transferred them to third parties and that she would not do so in the future. In addition, the savings bank had taken disciplinary measures against her.

The savings bank nevertheless notified the Land Hessen's Commissioner for Data Protection of this breach. After incidentally becoming aware of this breach, the customer lodged a complaint with that Commissioner for Data Protection. After hearing the savings bank, the Commissioner for Data Protection informed the customer that it did not consider it necessary to exercise any corrective powers in respect of the savings bank. The customer then brought an action before a German court, asking it to order the Commissioner for Data Protection to take action against the savings bank and, in particular, to impose on it a fine.

The German court has asked the Court of Justice to interpret the General Data Protection Regulation (GDPR) in this respect. The Court answers that when a breach of personal data has been established, the supervisory authority is not obliged to exercise a corrective power, in particular the power to impose an administrative fine, where this is not necessary to remedy the shortcoming found and to ensure that the GDPR is fully enforced. This could be the case, inter alia, where, as soon as the controller became aware of the breach, it took the necessary measures to ensure that that breach was brought to an end and did not recur.

The GDPR leaves the supervisory authority a discretion as to the manner in which it must remedy the shortcoming found. That discretion is limited by the need to ensure a consistent and high level of protection

of personal data through strong enforcement of the GDPR. It is for the German court to ascertain whether the Commissioner for Data Protection complied with those limits.

ARTIFICIAL INTELLIGENCE.

25 September 2024 – EU Commission: over a hundred companies sign EU AI Pact pledges to drive trustworthy and safe AI development.

The EU Commission announced over a hundred companies that are the first signatories of the EU artificial intelligence (AI) Pact and its voluntary pledges. The signatories include multinational corporations and European small and medium enterprises (SMEs) from diverse sectors, including IT, telecoms, healthcare, banking, automotive, and aeronautics. The Pact supports industry's voluntary commitments to start applying the principles of the AI Act ahead of its entry into application and enhances engagement between the EU AI Office and all relevant stakeholders, including industry, civil society and academia.

The EU AI Pact voluntary pledges call on participating companies to commit to at least three core actions:

- **AI governance strategy** to foster the uptake of AI in the organisation and work towards future compliance with the AI Act.
- **High-risk AI systems mapping**: Identifying AI systems likely to be categorised as high-risk under the AI Act
- **Promoting AI literacy and awareness among staff**, ensuring ethical and responsible AI development.

In addition to these core commitments, more than half of the signatories committed to additional pledges, including ensuring human oversight, mitigating risks, and transparently labelling certain types of AI-generated content, such as deepfakes.

Alongside the efforts to help companies implement the AI Act in anticipation of the legal deadline, the Commission is taking action to boost EU innovation in AI. The AI Factories initiative of 10 September 2024 will provide start-ups and industry with a one-stop-shop to innovate and develop AI, including data, talent and computing power. The AI Factories will also propel the development and validation of AI industrial and scientific applications in key European sectors such as healthcare, energy, automotive and transport, defence and aerospace, robotics and manufacturing, clean and agritech.

AI Factories are a highlight of the Commission's AI innovation package presented in January 2024, together with venture capital and equity support measures, the deployment of Common European Data Spaces, the 'GenAI4EU' initiative, and the Large AI Grand Challenge giving start-ups financial support and access to EU's supercomputers, among other measures. The Commission will also set up a European AI Research Council to exploit the potential of data, and the Apply AI Strategy to boost new industrial uses of AI.

---

25 September 2024 – EU Commission: Code of practice for general-purpose artificial intelligence shall be adopted within April 2025.

The EU Commission received almost 430 submissions in response to its multi-stakeholder consultation on the upcoming *Code of Practice for general-purpose artificial intelligence (GPAI*), as provided for by the AI Act.

The submissions received will inform Commission's work to finalise the Code of Practice by April 2025. The provisions in the AI Act on GPAI will enter into application 12 months after the Act's entry into force on 1 August 2025.

Key focus areas for the Code include transparency, copyright-related rules, risk assessment and mitigation, and related internal governance. Additionally, the input received will help guide the work of the AI Office, which will oversee the implementation and enforcement of the AI Act rules on GPAI. This input

will also be used by the AI Office to develop a template and guidelines for summarising training data used in GPAI models.

The consultation forms part of the Commission's broader efforts to promote the responsible development of artificial intelligence. Contributions were submitted by a diverse range of stakeholders, including GPAI providers, downstream providers, industry organisations, academia, civil society, rights holders, and other relevant groups, all offering varied perspectives on how to ensure trustworthy and responsible AI within the EU.

The consultation came in addition to a call for expressions of interest to participate in drawing-up the first Code of Practice for General-Purpose AI, which attracted almost 1000 organisations and individuals worldwide. The kick-off plenary will be held online on 30 September.

Find out more information about the multi-stakeholder consultation on the upcoming Code of Practice for general-purpose artificial intelligence (GPAI) and the AI Act.

---

24 September 2024 – Europol published a report on the benefits and challenges of artificial intelligence (AI) for law enforcement.

A new Europol report titled "*AI and Policing*" sheds light on how technologies utilizing artificial intelligence, particularly facial recognition, are being integrated into law enforcement, while concerns about privacy and civil rights grow.

Europol's assessment highlights the potential benefits AI can bring to policing, through the use of predictive policing, and the analysis of large datasets in real-time.

AI, according to the report, is transforming how police forces operate. AI tools, including facial recognition, are being used to streamline crime prevention, speed up investigations, and assist in identifying criminal networks, as well as locating missing persons and children by matching unidentified individuals' images against databases of those reported missing. However, the adoption of AI has raised ethical and legal questions, and concerns around bias in particular.

In the Europol report, law enforcement agencies are increasingly relying on AI-powered technologies like data analytics, pattern recognition, and decision-making systems. These systems help law enforcement enhance crime detection and prevention. AI's ability to analyse data from various sources, such as CCTV footage and social media, can provide police with crucial leads, the report highlights.

However, Europol emphasizes the necessity of balancing the technology with accountability and transparency. As AI systems become more prevalent, concerns about bias, misuse of personal data, and infringement on individual rights have surged. Europol underscores the importance of ethical frameworks and regulatory oversight so that AI-driven policing does not infringe on civil liberties.

DIGITAL MARKETS

25 September 2024 - G7 Cyber Expert Group Recommends Action to Combat Financial Sector Risks from Quantum Computing.

---

he G7 Cyber Expert Group (CEG) released a public statement highlighting the potential cybersecurity risks associated with developments in quantum computing and recommending steps for financial authorities and institutions to take to address those risks.

The G7 CEG's membership includes representatives of financial authorities across all G7 countries as well as the European Union. It was founded in 2015 to serve as a multi-year working group that coordinates cybersecurity policy and strategy across the member jurisdictions.

Quantum computers are being built that will be able to solve computational problems currently deemed impossible for conventional computers to solve within a reasonable amount of time. While potentially providing significant benefits to the financial system, these powerful computers will also carry with them unique cybersecurity risks. One of the most significant is that cyber threat actors could use quantum computers to defeat certain cryptographic techniques that secure communications and IT systems, potentially exposing financial entity data, including customer information.

While the exact timeline for developing quantum computers with these capabilities is uncertain, there is a real possibility that such capabilities could emerge within a decade. These quantum computers would not only put future data at risk, but also any previously transmitted data that cyber adversaries have been able to intercept and store with the intent of decrypting later with quantum computers. Due to the potentially long lead time needed to put in place quantum-resilient technologies, the time to start planning is now.

An initial set of quantum-resilient encryption standards was released by the National Institute of Standards and Technology (NIST) last month. Additional standards from NIST and other standard-setting bodies are expected in the future. It is important for financial entities to maintain the agility required to incorporate new encryption standards in a timely and appropriate manner as they become available.

With the availability of NIST's standards, some financial entities may be in a position now to start making the needed changes to implement quantum resilient technologies within their systems. Others may be dependent on vendors and other third parties to develop implementations of the new standards that can be incorporated once they become available. No matter where entities are in their adoption timelines, the G7 CEG strongly encourages financial authorities and institutions to begin taking the following steps to build resilience against quantum computing risks:

1. Develop a better understanding of the issue, the risks involved, and strategies for mitigating those risks
2. Assess quantum computing risks in their areas of responsibility.
3. Develop a plan for mitigating quantum computing risks.

The CEG statement provides additional details on quantum computing risks and the specific actions that financial entities can start taking to build quantum resilience within the financial system.

INFORMATION TECHNOLOGY

25 September 2024 – Legislative Decree No. 134 of 4 September 2024 on 'Implementation of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical players' published in the Official Gazette.

With the Directive (EU) 2022/2557 (*ERC Directive*) action is taken to:

- achieve an appropriate level of harmonisation in the identification of sectors, sub-sectors and categories of actors that qualify as critical;
- strengthen their resilience, understood as their ability to prevent, protect, respond to, mitigate, absorb, adapt to and restore their operational capabilities following incidents that may disrupt the provision of essential services.

Critical Entity: a public or private entity identified within the categories of entities operating in the sectors and sub-sectors set out in Annex A of this provision. Critical Entities are identified in at least the following sectors:

- energy;
- transport;
- banking;
- financial market infrastructure;
- health;

- drinking water;
- waste water;
- digital infrastructure;
- space;
- food production, processing and distribution;
- public administration bodies.

Specifically, Legislative Decree No. 134/2024 establishes:

- measures to ensure that services that are essential for the maintenance of vital societal functions, economic activities, public health and safety, or the environment are provided without hindrance, as well as criteria for the identification of critical actors;
- obligations on critical actors to strengthen their resilience, to a high level, and to enhance their ability to provide essential services, in the internal market, in order to improve their functioning;
- measures to support the fulfilment of obligations imposed on critical actors;
- provisions regarding the supervision and imposition of sanctions on critical actors;
- Provisions regarding the identification of critical actors of particular European relevance and the European Commission's advisory missions to assess the measures put in place by these actors to fulfil their obligations;
- provisions for the preparation of the *National Strategy for Critical Subject Resilience*;
- the regulation of risk assessment by the State and risk assessment by critical actors;
- the establishment of the Inter-Ministerial Resilience Committee, as well as the identification of the relevant sectoral authorities and the single point of contact;
- the modalities of cooperation with other Member States and the European Commission, including national participation in the critical actors resilience group.

Critical actors' resilience measures.

Critical actors should take and apply appropriate and proportionate technical, security and organisational measures to ensure their own resilience, based on the relevant State risk assessment information provided by the PCU.

The single point of contact (PCU), established within the Presidency of the Council of Ministers, has the functions of:

o ensuring liaison with the European Commission and cooperation with third countries;

o coordinating activities to support critical actors in strengthening their resilience;

o receiving notifications from critical actors, at the same time as the competent authorities, of incidents that disrupt or may significantly disrupt the provision of essential services;

o promote research and training activities on critical infrastructure resilience.