FIVERS

Regulatory update
Data protection, AI, IT and IP

n. 7 / 2024

DATA PROTECTION

25 July 2024 – EU Commission: second report on GDPR enforcement published.

---

25 July 2024 - EU Court of Justice: failure to provide privacy information notice is a breach entitling representative associations to bring actions - even without a mandate from the data subject - under Article 80(2) GDPR.

---

22 July 2024 – EU Commission coordinates action by national consumer protection authorities against Meta on "pay or consent" model.

---

22 July 2024 – IAB Europe outlines concerns regarding GDPR procedural regulation.

---

22 July 2024 – Italian Data Protection Authority launches investigations into the effects of the Crowdstrike computer blackout.

---

18 July 2024 – Council of Europe: publication of the Arabic Version of the Handbook on European Data Protection Law.

ARTIFICIAL INTELLIGENCE.

22 July 2024 – EU Commission publishes draft AI Pact.

---

22 July 2024 – The Italian AI Committee adopts the Italian Strategy for Artificial Intelligence 2024-2026.

---

22 July 2024 – OECD announces pilot phase for G7 Hiroshima AI Process.

CYBERSECURITY

26 July 2024 - Italian National Security Agency (ACN) published a guide to reporting incidents to the Computer Security Incident Response Team Italy (CSIRT Italy).

---

22 July 2024 – Guidelines on encryption enacted by the National Agency for Cybersecurity.

INFORMATION TECHNOLOGY

26 July 2024 - Ministry of Justice: the electronic platform for the collection of digital signatures valid for abrogative or constitutional referendums and legislative initiatives of a popular nature is operational.

---

26 July 2024 – World Trade Organisation - WTO adopts agreement on e-commerce.

DATA PROTECTION

25 July 2024 – EU Commission: second report on GDPR enforcement published.

The European Commission found serious enforcement issues with the General Data Protection Regulation (GDPR) and called for clearer guidelines to strengthen data protection across member states in the second report published.

This is the EU Commission's second report on the application of the EU's GDPR, in force since 2018. The periodical report is required every four years, starting from 2020 and the EU Commission should publish reviews of the GDPR to identify any issues, possibly leading to amendments to the regulation. The first one was published two years ago.

In particular, the report highlighted a significant uptick in enforcement activity by data protection authorities in recent years including landmark fines for:

- the infringement of the lawfulness and security of processing;
- the infringement of processing of special categories of personal data; and
- the failure to comply with individuals' rights.

Regarding data protection authorities, the report noted the increased resources for data protection authorities in terms of budget and staff. However, data protection authorities have been noted to struggle in handling high numbers of consumer complaints and adopt divergent interpretations of the GDPR. The report detailed the fragmented application of the GDPR in areas such as the minimum age for a child's consent, the introduction of further conditions for processing genetic data, biometric data, and health data, and the processing of personal data relating to criminal convictions and offenses.

On data subject rights, the report provided that the right of access is the most frequently right exercised by data subjects, though challenges remain in interpreting when requests are unfounded or excessive. The report also noted the increased use of the right to data portability, which was facilitated by the requirement under the Digital Markets Act (DMA) for 'gatekeepers' to provide effective portability of users' data. On the exercise of data subjects' rights by children, the report considered that children did not fully understand their rights.

The report further addressed the data protection challenges faced by small and medium sized enterprises (SME). This includes the role of a Data Protection Officer (DPO), where SMEs have faced challenges including:

- appointment of DPOs with requisite experience;
- lack of EU-wide standards for education and training;
- failing to adequately integrate DPOs;
- lack of resources;
- other tasks outside data protection; and
- insufficient seniority.

Notably, the report considers the data transfer landscape, providing that adequacy decisions in particular have facilitated data flows. The report noted that adequacy decisions adopted by the Commission are increasingly relevant since jurisdictions with adequate status are recognized by other jurisdictions as safe destinations under their own data protection rules. Although the report acknowledges that data exporters are struggling with transfer impact assessments, the EU standard contractual clauses (SCC) and binding corporate rules (BCR) are still widely used. The adoption of model clauses by other jurisdictions has also increased the scale of cross-border data flows.

The report considers that to ensure strong protection for individuals and ensure the free flow of personal data within and outside the EU, there is a need to focus on, among other things:

proactive support by data protection authorities in compliance efforts;
- consistent application of the GDPR across the EU;
- effective cooperation between data protection authorities;
- establishing cooperation with sectoral regulators on issues with an impact on data protection; and
- implementing efficient and targeted working arrangements for guidelines, opinions, and decisions, and prioritizing key issues to reduce the burden on data protection authorities.

---

25 July 2024 - EU Court of Justice: failure to provide privacy information notice is a breach entitling representative associations to bring actions - even without a mandate from the data subject - under Article 80(2) GDPR.

The Bundesgerichtshof (Federal Court of Justice, Germany) referred a question to the CJEU for a preliminary ruling on the interpretation of Article 80(2) of the GDPR. According to that provision, Member States may provide that a body, organisation or association, irrespective of the mandate given by the data subject, has the right to lodge a complaint with the supervisory authority in the Member State in question, pursuant to Article 77 of the GDPR, and to exercise the rights provided for in Articles 78 and 79 thereof, if it considers that the rights enjoyed by a data subject under that regulation have been infringed as a result of 'the processing of personal data'.

The reference for a preliminary ruling was made in the context of a dispute in Germany between Meta and the Federal Union of German Consumer Organisations and Associations concerning Meta Platforms Ireland's alleged infringement of the German legislation on the protection of personal data, which constitutes, at the same time, an unfair commercial practice, an infringement of a consumer protection law and a breach of the prohibition on the use of invalid general terms and conditions.
In that action, the referring court expressed doubts as to the admissibility of the Federal Union's action. It wondered, in particular, whether the Federal Union's legal standing could derive from Article 80(2) of the GDPR even in the case of a mere failure by the controller to provide information about the processing pursuant to Articles 12 and 13 of the GDPR. That is why it referred a question to the CJEU for a preliminary ruling on the interpretation of that provision.

The CJEU concluded that Article 80(2) of the HGDPR must be interpreted as meaning that the condition that a qualified entity, in order to bring a representative action under that provision, must allege that a data subject's rights under that regulation have been infringed 'as a result of the processing', within the meaning of that provision, is satisfied where that entity alleges that the infringement of that person's rights occurs 'as a result of the processing' of personal data and that it results from the controller's failure to fulfil its obligations under Article 12 first sentence of Article 12(1) and of Article 13(1)(c) and (e) of that regulation, to communicate to the person concerned by that processing of data, in a concise, transparent, intelligible and easily accessible form, in plain and intelligible language, the information relating to the purpose of that processing of data and to the recipients of those data, at the latest at the time of the collection of those data.

---

22 July 2024 – EU Commission coordinates action by national consumer protection authorities against Meta on "pay or consent" model.

The Consumer Protection Cooperation (CPC) Network sent a letter following concerns that Meta's 'pay or consent' model might breach EU consumer law. The EU Commission coordinated this action which is led by the French Directorate General for Competition, Consumer Affairs and Fraud Prevention. The action started in 2023, immediately after Meta had requested consumers overnight to either subscribe to use Facebook and Instagram against a fee or to consent to Meta's use of their personal data to be shown personalised ads, allowing Meta to make revenue out of it ('pay or consent').

Consumer protection authorities assessed several elements that could constitute misleading or aggressive practices, in particular whether Meta provided consumers upfront with true, clear and sufficient information. They analysed whether this information allowed consumers to understand the implications of their decision

to pay or to accept the processing of their personal data for commercial purposes on their rights as consumers. In addition, CPC authorities are concerned that many consumers might have been exposed to undue pressure to choose rapidly between the two models, fearing that they would instantly lose access to their accounts and their network of contacts.

This coordinated action by the CPC network against Meta comes on top of other ongoing EU and national procedures related to the same model. This action focuses specifically on the assessment of Meta's practices under EU consumer law and is distinct from the ongoing investigations against the company by the Commission on its 'pay or consent' model potentially breaching the Digital Markets Act (DMA), the Commission's formal request for information under the Digital Services Act (DSA), and the assessment by the Irish Data Protection Commission under the General Data Protection Regulation (GDPR).

CPC authorities identified several practices in the context of Meta's roll-out of its new business model that raise concern and could potentially be considered unfair and contrary to the Unfair Commercial Practices Directive (UCPD) and the Unfair Contract Terms Directive (UCTD):

- Misleading consumers by using the word 'free' while, for users who do not want to subscribe against a fee, Meta requires them to accept that Meta can make revenue from using their personal data to show them personalised ads;
- Confusing users by requiring them to navigate through different screens in the Facebook/Instagram app or web-version and to click on hyperlinks directing them to different parts of the Terms of Service or Privacy Policy to find out how their preferences, personal data, and user-generated data will be used by Meta to show them personalised ads;
- Using imprecise terms and language, such as 'your info' to refer to consumers' 'personal data' or suggesting that consumers who decide to pay will not see ads at all, while they might still see ads when engaging with content shared via Facebook or Instagram by other members of the platform;
- Pressurising consumers who have always used Facebook/Instagram free of charge until the new business model was introduced, and for whom Facebook/Instagram often constitute a significant part of their social lives and interactions to make an immediate choice, without giving them a pre-warning, sufficient time, and a real opportunity to assess how that choice might affect their contractual relationship with Meta, by not letting them access their accounts before making their choice.

Meta has until 1 September 2024 to reply to the letter of the CPC network and the EU Commission and to propose solutions. If Meta does not take the necessary steps to solve the concerns raised, CPC authorities can decide to take enforcement measures, including sanctions.

---

22 July 2024 – IAB Europe outlines concerns regarding GDPR procedural regulation.

The Interactive Advertising Bureau (IAB) Europe released a comprehensive paper outlining significant concerns regarding the European Parliament and European Council positions on the General Data Protection Regulation (GDPR) procedural regulation.

The IAB outlined a number of areas of concern, including:

- the need for early resolution mechanisms and complaint admissibility to expedite complaint resolutions and reduce administrative delays, which are currently leading to significant backlogs;
- the importance of maintaining the One-Stop-Shop mechanism, which ensures consistent application of the GDPR across different jurisdictions;
- concerns over the weakening of business information confidentiality protections, which could lead to media leaks and compromise the independence of supervisory authorities; and

- the need to ensure uniform application of the right to be heard across Europe, allowing parties under investigation to effectively express their views during administrative procedures and avoid legal uncertainty.

---

22 July 2024 – Italian Data Protection Authority launches investigations into the effects of the Crowdstrike computer blackout.

The Italian Data Protection Authority, on the basis of data breach notifications received, has launched investigations into the consequences that the recent computer system blackout may have had on users' personal data, particularly when using public services.

The event resulted from a malfunction of the CrowdStrike security software that blocked the operation of numerous online services in recent days.

---

18 July 2024 – Council of Europe: publication of the Arabic Version of the Handbook on European Data Protection Law.

As part of a longstanding cooperation between the European Union Agency for Fundamental Rights (FRA) and the Council of Europe, the "Handbook on European Data Protection Law" has been translated into Arabic. This handbook was jointly developed, and is published, by the Council of Europe, the European Court of Human Rights (ECHR), and the FRA.

The translation of the handbook into Arabic aims to foster a common legal framework across the Mediterranean and to enable interested parties, particularly legal professionals in the southern Mediterranean countries, to deepen their understanding of human rights in relation to privacy and personal data protection.

The translation will facilitate the introduction of reforms and the adoption of personal data protection laws in the countries in the region.

This initiative is supported by the joint programme between the Council of Europe and the European Union, "Protecting Human Rights, Rule of Law and Democracy through Shared Standards in the Southern Mediterranean" (South Programme V), co-financed by both organisations and implemented by the Council of Europe.

ARTIFICIAL INTELLIGENCE.

22 July 2024 – EU Commission publishes draft AI Pact.

The European Commission published the draft AI Pact pursuant to the EU Artificial Intelligence Act (the EU AI Act).

The draft AI Pact is a voluntary commitment anticipating the requirements under the EU AI Act, implementing them before legal deadlines. The draft AI Pact has received responses from over 550 organizations.

The Commission outlined that the draft AI Pact is centered around the following two pillars:

Pillar I - as a gateway to engage the AI Pact network, encouraging the exchange of best practices, and providing practical information on the implementation of the EU AI Act through:

- the organization workshops; and
- creating and managing a dedicated online space for exchanging best practices; and

Pillar II - to encourage AI system providers and deployers to prepare early and take action for compliance with requirements and obligations set out under the EU AI Act through:

- the creation of templates and monitoring schemes;
- pledges to take concrete actions on the EU AI Act's requirements, functioning as incremental objectives; and
- reporting commitments on a regular basis, with commitments published by the AI Office for visibility, accountability, and credibility.

Organizations can contribute to the draft AI Pact here.

---

22 July 2024 – The Italian AI Committee adopts the Italian Strategy for Artificial Intelligence 2024-2026.

A few days after the publication of the EU Regulation on AI no. 2024/1689 in the Official Journal of the European Union and the beginning of the hearings in committee, at the Senate of the Republic, of the Italian Government's bill on artificial intelligence, the full document of the Italian Strategy for Artificial Intelligence 2024-2026 is available online.

The text was drafted by the Committee of Experts to support the Government in defining national legislation and strategies related to this technology. The document reflects the Government's commitment to creating an environment in which AI can develop in a safe, ethical and inclusive manner, maximising benefits and minimising potential adverse effects.

After an analysis of the global context and Italy's positioning, the document defines strategic actions, grouped into four macro-areas: Research, Public Administration, Enterprise and Training. The strategy also proposes a system for monitoring its implementation and an analysis of the regulatory context that outlines the framework within which it is to be deployed.

---

22 July 2024 – OECD announces pilot phase for G7 Hiroshima AI Process.

The OECD - Organization for Economic Cooperation and Development announced a pilot phase to monitor the application of the Hiroshima Process International Code of Conduct for Organizations Developing AI Systems (G7 Hiroshima AI Process). The OECD clarified that the *G7 Hiroshima AI Process* is a comprehensive policy framework on artificial intelligence (AI) consisting of:

- the OECD's Report towards a G7 Common Understanding on Generative AI;
- International Guiding Principles;
- International Code of Conduct; and
- project-based cooperation on AI.

The pilot phase is open to participation here until September 6, 2024, and is open to input from organizations developing advanced AI systems. The pilot aims to establish a monitoring mechanism for the Code of Conduct.

The Code of Conduct provides 11 Principles including:

- taking appropriate measures to identify, evaluate, and mitigate risks throughout the AI lifecycle;
- monitoring for patterns of misuse, after deployment, including placement on the market;
- publicly reporting advanced AI systems' capabilities, limitations, and domains of appropriate and inappropriate use, to support transparency;
- working towards information sharing and reporting of incidents among organizations developing advanced AI systems;
- developing, implementing, and disclosing AI governance and risk management policies;
- investing in and implementing robust security controls, including physical measures;

- developing and deploying reliable content authentication and provenance mechanisms where technically feasible;
- prioritizing research to mitigate societal, safety, and security risks;
- prioritizing the development of advanced AI systems to address global challenges including climate, health, and education;
- advancing the development and adoption of international technical standards; and
- implementing appropriate data input measures, protection for personal data, and intellectual property.

CYBERSECURITY

26 July 2024 - Italian National Security Agency (ACN) published a guide to reporting incidents to the Computer Security Incident Response Team Italy (CSIRT Italy).

The guide provides instructions to both public and private entities, entities included in the National Cyber Security Perimeter (PSNC), and those operating in the network and information systems and telecommunications sector.

The guide outlines the following four phases:

- the preparatory phase - which involves collecting the minimum information needed to guarantee sufficient knowledge of the event;
- the incident reporting phase - which involves filling out a form on the CSIRT Italy's website within a timeframe;
- the management of the notification by CSIRT Italy to provide support to victims; and
- the incident closure phase.

You can read the press release here.

---

22 July 2024 – Guidelines on encryption enacted by the National Agency for Cybersecurity.

Encryption allows you to secure communications in the digital world in a secure and efficient way. After the guidelines on password retention, hash functions and message authentication codes, the National Cybersecurity Agency, ACN, publishes other insights on cryptography dedicated to data confidentiality and quantum threat preparedness techniques.

From the introductory document to the indications on block ciphers, which is one of the most important tools to ensure the confidentiality of data, the new documents help to orient oneself among the specifications of cryptographic algorithms and to better understand the operation of ciphers and the interaction with the messages to be sent.

The first of the information documents that ACN makes available to learn more about cryptographic topics is also available. Unlike the "Guidelines for Cryptographic Functions", these documents are intended to inform and raise awareness on topics central to modern cryptography, providing a broad overview and including the most relevant information for the structures and institutions of our country. The first of the series is dedicated to "Post-quantum and quantum cryptography" for quantum threat preparedness and contains an overview of the current scenario, useful for considering the main post-quantum or quantum alternatives and developments at the international level.

Among the guidelines already published in December 2023 are indications for the storage of passwords, created together with the Guarantor for the protection of personal data and which concern the way in which the provider of the service being accessed must protect the password to access it; indications on cryptographic hash functions, fundamental tools for cybersecurity because, thanks to their properties, they make it possible to ensure the integrity of data, i.e. they allow you to verify the alteration of a piece of data or a message; and message authentication codes or MACs, which help ensure the integrity of a message and verify the identity of the sender.

The guidelines and information documents are part of a series of technical publications that serve to protect the cyberspace in which we all move. Together, these guidelines provide precise indications for the use of cryptographic algorithms throughout the entire life cycle of ICT systems and services, in accordance with the principles of security and privacy protection. In each document, the last chapter contains the conclusions drawn from the dissertation carried out and the list of algorithms and parameters recommended by ACN.

Following the example of other international realities, the Technological Scrutiny and Cryptography Division, within the Certification and Supervision Service of the Agency, directed by Admiral Andrea Billet, has decided to start the publication of the series "Guidelines for Cryptographic Functions", which represent the main (primitive) cryptographic functions both from a theoretical and practical point of view.

The creation of these documents is part of the functions attributed to the National Cybersecurity Agency for the first time enshrined in Italian legislation (by Legislative Decree 82/2021), for which the ACN is a promoter of the use of cryptography as a cybersecurity tool, in implementation of measure #22 of the National Cybersecurity Strategy.

INFORMATION TECHNOLOGY

26 July 2024 - Ministry of Justice: the electronic platform for the collection of digital signatures valid for abrogative or constitutional referendums and legislative initiatives of a popular nature is operational.

The D.P.C.M. (Prime Ministerial Decree) of 18 July 2024 was published in the Official Gazette No. 173/2024 on 'Certification of the operativeness of the Platform for the collection of signatures for referendums, referred to in Article 1, paragraphs 341 et seq. of Law No. 178 of 30 December 2020', which provides for the activation of the new digital platform dedicated to the collection of signatures for referendums.

The platform is designed to facilitate the digital signature of abrogative or constitutional referendums and legislative initiatives of a popular nature. Its activation is provided for in the Prime Ministerial Decree of 18 July 2024, published in Official Gazette No. 173/2024.

The system has obtained the opinion of the Italian Data Protection Authority and can be used by the promoters of referendum proposals and by the offices of the Supreme Court and the Chambers to manage all the stages of the process of collecting signatures of supporters in digital format. The system then verifies the presence and validity of the signatures, through interoperability with the National Register of Resident Population (ANPR) system, at the registry offices of the municipalities where the citizens who signed the proposals are resident.

---

26 July 2024 – World Trade Organisation - WTO adopts agreement on e-commerce.

The World Trade Organization (WTO) announced the adoption of the Agreement on Electronic Commerce which shall apply to measures adopted or maintained by a party affecting trade by electronic means.

However, the Agreement does not apply to:

- government procurement.
- a service supplied in the exercise of governmental authority; or
- except for Articles 8, 9, and 12 of the Agreement, information held or processed by or on behalf of a party, or measures related to that information, including measures related to its collection.

The Agreement contains provisions in relation to trust and e-commerce, including personal data protection, unsolicited electronic communication, and cybersecurity, among other things.

The Agreement states that a party must adopt or maintain measures that, among other things:

- require suppliers of commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages;
- require the consent, as specified in its laws or regulations, of recipients to receive commercial electronic messages; or
- provide for the minimization of unsolicited commercial electronic messages.

The Agreement also requires each party to adopt or maintain a legal framework that provides for the personal data protection of e-commerce users. Additionally, the Agreement states that each party must publish information on the personal data protections it provides to users of electronic commerce, including guidance on how a natural person can pursue remedies and how enterprises can comply with legal requirements.

Any member of the WTO may accept this Agreement. Acceptance shall take place by deposit of an instrument of acceptance to this Agreement with the Director-General of the WTO. The Agreement will enter into force on the 30th day following the date of deposit of the instrument of acceptance.