FIVERS

Regulatory update
Data protection, AI, IT and IP

n. 10 / 2024

DATA PROTECTION

16 September 2024 - Italian Data Protection Authority: favourable opinion on the legislative decree scheme transposing EU Directive 2022/2557 on the resilience of critical entities.

---

12 September 2024 – EU Court of Justice: interpretation of the basis of lawfulness of processing represented by the performance of a contract, or legal obligation and the pursuit of legitimate interest in the case of disclosure of personal data of investment fund partners.

---

11 September 2024 - EU: Commission plans public consultation on standard contractual clauses (SCCs) for the transfer of data to third country controllers and processors subject to the GDPR.

---

10 September 2024 - EDPB to work together with European Commission to develop guidance on interplay GDPR and DMA.

ARTIFICIAL INTELLIGENCE.

10 September 2024 - Artificial Intelligence Board kicks off work on uptake of AI in the EU and implementation of the AI Act.

---

5 September 2024 – Council of Europe opens first ever global treaty on AI for signature.

---

5 September 2024 – Council of Europe publishes a report on the regulatory approaches to Artificial Intelligence in Finance.

DIGITAL MARKETS

16 September 2024 - Legislative Decree No. 129/2024 adapting national legislation to MiCAR Regulation (EU) 2023/1114 published in the Italian Official Gazette.

---

6 September 2024 - EU Commission: explanatory FAQs for Regulation 2054/2023 (Data Act) released.

INFORMATION TECHNOLOGY

10 September 2024 - Court of Cassation: electronic serving occurs when the receipt of acceptance is generated.

CYBERSECURITY

6 September 2024 – National Cybersecurity Agency: the Presidential Decree for the allocation of funds in the three-year period 2024 - 2026 within the National Cyber Security Strategy published.

DATA PROTECTION

September 16, 2024 - Italian Data Protection Authority: favorable opinion on the legislative decree scheme transposing EU Directive 2022/2557 on the resilience of critical entities.

Favourable opinion of the Italian Data Protection Authority on the legislative decree scheme transposing the European Directive on the resilience of critical entities (CER Directive - critical entities resilience), operating in particularly sensitive sectors (energy, health, digital infrastructure, PA).
The draft legislative decree provides, among other things, for the introduction of measures, criteria, obligations, sanctions and provisions aimed at ensuring the provision of essential services for the maintenance of vital functions of society or economic activities, public health and safety or the environment.

In providing its opinion to the Italian Government, the Authority considered that the draft legislative decree, while not presenting any particular critical issues from a data protection standpoint, needs some additions regarding the verification of criminal records for those who hold sensitive roles within facilities.
In particular, the Authority has asked to specify which categories of (essentially criminal) records are considered "relevant" and to regulate the manner and timeframe in which certificates of European criminal records acquired are kept, possibly also deferring to the regulatory source.

It should then be considered, according to the Authority, whether it would be appropriate to supplement the outline by recalling the requirements in cases where particular events or incidents involve personal data breaches.

---

12 September 2024 – EU Court of Justice: interpretation of the basis of lawfulness of processing represented by the performance of a contract, or legal obligation and the pursuit of legitimate interest in the case of disclosure of personal data of investment fund partners.

The EU Court of Justice issued an important preliminary ruling (2024/738) on the proper application of Articles 6(1)(b) and 6(1)(f) of the EU General Data Protection Regulation 679/2016. These are the bases of lawfulness of processing represented by the fulfilment of contractual obligations, of a legal obligation and the pursuit of legitimate interest, either one's own or that of a third party.

The case: at the request of a partner of an investment fund established in the form of a partnership offering shares for public subscription, information on all the partners with indirect shareholdings in that fund, through trust companies, irrespective of the size of their shareholding in the capital of those funds, should have been disclosed by the Data Controller for the purpose of contacting them and negotiating the purchase of their shares or to coordinate with them for the purpose of reaching a consensus in connection with partners' resolutions.
The EU Court held that the processing represented by the disclosure of partners' personal data may be regarded as being necessary, within the meaning of article 6(1)(b), for the performance of the contract pursuant to which those partners have purchased such shareholdings, only on condition that that processing is objectively indispensable for a purpose that is integral to the contractual obligation intended for those same partners, with the result that the main subject matter of the contract could not be achieved if that processing were not to occur. That is not the case if that contract expressly prohibits the disclosure of those personal data to other shareholders.

With regard to the pursuit of legitimate interest under Article 6(1)(f) of the GDPR, the CJEU has held that the processing represented by the disclosure of personal data of the partners may be regarded as being necessary for the purposes of legitimate interests pursued by a third party, within the meaning of art. 6(1)(f), only on condition that that processing is strictly necessary to achieve such a legitimate interest and that, in the light of all the relevant circumstances, the interests or fundamental rights and freedoms of those partners do not override that legitimate interest..

As for the fulfilment of a legal obligation under Article 6(1)(c) of the GDPR, the CJEU has held that the processing of personal data is justified, under that provision, where it is necessary for compliance with a legal obligation to which the controller is subject, under the law of the Member State concerned, as stated by the case-law of that Member State, on condition that that case-law is clear and precise, that its application is foreseeable for those persons subject to it and that it meets an objective of public interest and is proportionate to it.

---

11 September 2024 - EU: Commission plans public consultation on standard contractual clauses (SCCs) for the transfer of data to third country controllers and processors subject to the GDPR.

The European Commission announced that it plans to request public feedback on Standard Contractual Clauses (SCCs) under the General Data Protection Regulation (GDPR) in the fourth quarter of 2024. Standard contractual clauses are model data protection clauses EU data exporters can incorporate into their contracts to transfer personal data to data importers in third countries in line with the requirements of the General Data Protection Regulation (GDPR). These clauses are for the specific case where a data importer is located in a third country but is directly subject to the GDPR. They complement the existing clauses, for data transfers to third country importers not subject to the GDPR.

---

10 September 2024 - EDPB to work together with European Commission to develop guidance on interplay GDPR and DMA.

The Commission services in charge of the enforcement of the Digital Markets Act (DMA) and the European Data Protection Board (EDPB) have agreed to work together to clarify and give guidance on the interplay between DMA and GDPR.

This enhanced dialogue between Commission's services and the EDPB will focus on the applicable obligations to digital gatekeepers under the DMA which present a strong interplay with the GDPR, as there is a need to ensure the coherent application to digital gatekeepers of the applicable regulatory frameworks.

Developing a coherent interpretation of the DMA and GDPR while respecting each regulators' competences in areas where the GDPR applies and is referenced in the DMA is crucial to effectively implement the two regulatory frameworks and achieve their respective and complementary objectives.

The DMA established a High Level Group to provide the Commission with advice and expertise to ensure that the DMA and other sectoral regulations applicable to gatekeepers are implemented in a coherent and complementary manner. The Commission and representatives from the EDPB and EDPS already engaged on data-related and interoperability obligations in the High Level Group. This project builds on this engagement and deepens the cooperation in relation to the two specific regulatory frameworks.

ARTIFICIAL INTELLIGENCE.

10 September 2024 - Artificial Intelligence Board kicks off work on uptake of AI in the EU and implementation of the AI Act.

The Commission is hosting the first official meeting of the Artificial Intelligence (AI) Board, following the entry into force of the AI Act on 1st August.

This inaugural session, which takes place in Brussels, marks an important step in the EU's commitment to shape a robust framework for AI governance.

The AI Board is comprised of high-level representatives from the Commission and all EU Member States, and is discussing how to enhance the development and uptake of AI in the EU and the next steps in the implementation of the AI Act. The European Data Protection Supervisor (EDPS) and EEA/EFTA representatives from Norway, Liechtenstein, and Iceland are participating as observers. The EU AI Office provides the Secretariat for the AI Board.

The meeting is primarily focusing on the following key areas: the establishment of the AI Board's organisation and the adoption of its rules of procedure; an update and strategic discussion on EU AI policy, including the GenAI4EU initiative and international AI activities; a progress update and discussion on the first deliverables of the Commission related to the AI Act's implementation; and an exchange of best practices for national approaches to AI governance and AI Act implementation.

---

5 September 2024 – Council of Europe opens first ever global treaty on AI for signature.

The Council of Europe Framework Convention on artificial intelligence and human rights, democracy, and the rule of law (CETS No. 225) was opened for signature during a conference of Council of Europe Ministers of Justice in Vilnius. It is the first-ever international legally binding treaty aimed at ensuring that the use of AI systems is fully consistent with human rights, democracy and the rule of law.

The Framework Convention was signed by Andorra, Georgia, Iceland, Norway, the Republic of Moldova, San Marino, the United Kingdom as well as Israel, the United States of America and the European Union.

The treaty provides a legal framework covering the entire lifecycle of AI systems. It promotes AI progress and innovation, while managing the risks it may pose to human rights, democracy and the rule of law. To stand the test of time, it is technology-neutral.

The Framework Convention was adopted by the Council of Europe Committee of Ministers on 17 May 2024. The 46 Council of Europe member states, the European Union and 11 non-member states (Argentina, Australia, Canada, Costa Rica, the Holy See, Israel, Japan, Mexico, Peru, the United States of America and Uruguay) negotiated the treaty. Representatives of the private sector, civil society and academia contributed as observers.

The treaty will enter into force on the first day of the month following the expiration of a period of three months after the date on which five signatories, including at least three Council of Europe member states, have ratified it. Countries from all over the world will be eligible to join it and commit to complying with its provisions.

---

5 September 2024 – Council of Europe publishes a report on the regulatory approaches to Artificial Intelligence in Finance.

The Organisation for Economic Cooperation and Development (OECD) announced the publication of a policy paper on the regulatory approaches to artificial intelligence (AI) in finance. The policy paper, among

other things, analyses different regulatory approaches to the use of AI in finance in 49 OECD and non-OECD jurisdictions based on the survey on regulatory approaches to AI in finance.

The vast majority of respondents reported that they have appropriate regulation in place, while acknowledging that there may be some gaps and more general guidance may be valuable. The absence of explicit sectorial regulation for AI in finance in the majority of respondent jurisdictions could be (at least partially) explained by the fact that existing financial regulation, laws and guidance applies to financial activities regardless of the technology used. Where AI is used within areas for applications that are covered by existing rules or guidance, such rules or guidance should generally apply regardless of whether the decision came from AI (with or without human intervention), traditional models or humans. This includes, for example, general rules on prudent business, consumer/investor protection laws and regulations, guidance on model risk management, third-party risk management, disclosure requirements, handbooks related to IT governance, and cyber-security and operational resilience laws and regulations, as well as fairness laws, which continue to apply irrespective of the technology used. Advances in technology do not render existing safety and soundness standards and compliance requirements inapplicable. Many of the risks related to AI are not necessarily new or unique to AI innovation but rather exacerbated and amplified by the use of such innovation – or manifest in different ways.

The report is based on 49 responses to the OECD Survey on Regulatory Approaches to AI in Finance by 38 OECD countries (i.e. Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, United Kingdom, United States) as well as by 6 accession candidates to the OECD (i.e. Argentina, Brazil, Bulgaria, Croatia, Peru, Romania) and 4 non-OECD member jurisdictions (i.e. Hong Kong, China, Indonesia, Singapore, South Africa), as well as a consolidated answer provided by the EU Institutions (i.e. EC, EBA, EIOPA, ESMA) and was conducted in Q1 2024.

The majority of respondent jurisdictions have introduced some form of policy that covers AI in (parts of) finance, albeit in different forms: cross-sectorial legislation covering part of financial activity; binding rules or proposals issued by financial regulators, and non-binding policy guidance or clarifications released by financial regulators/supervisors. Importantly, these approaches are not mutually exclusive. For example, in jurisdictions with binding legislation covering parts of finance, existing sectorial regulation continues to apply without necessarily explicitly referencing AI and given the tech-neutral approach of OECD member countries. In particular, some respondents have introduced (or are in the process of introducing) legislation related solely to AI, such as for example Brazil, Chile, Colombia and Peru. These legislations are cross-sectorial and, in the case of the EU AI Act, have explicit provisions for specific parts of the financial sector. For example, the EU AI Act regulates AI-based creditworthiness assessments by banks, as well as pricing and risk assessments in life and health insurance with heightened requirements applying to these AI financial applications as they are considered high risk use cases. A small number of rules or proposed rules have also been introduced by financial regulators aiming at specific sectors or parts of the activities.

Non-binding policy guidance (e.g. principles, guidelines, white papers) on the use of AI has been reported in several respondent jurisdictions and is either explicitly targeting financial activity or are cross-sectorial and inclusive of financial activities. Such guidance can be government-led with blueprints or white papers covering all parts of economic activity, including finance (e.g. US President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence; or the UK Government's White Paper "A pro-innovation approach to AI Regulation"). Such guidance also encourages financial regulators to consider using their full range of authorities to protect consumers and investors from risks that may arise from the use of AI (e.g. the United States). Non-binding guidance has also been issued by financial regulators in some jurisdictions either providing broad recommendations for the use of AI in finance or focusing on specific areas of activity (e.g. Robo-advice services, creditworthiness assessment). Only a minority of financial regulators/supervisors in respondent jurisdictions have issued specific supervisory expectations or clarifications around the use of AI in finance. Some respondents have reported that, at the practical implementation level, there may be a need for additional regulatory/ supervisory guidance to assist authorised/supervised entities in their compliance, given unique issues arising in the deployment of AI innovation, depending on the case. Finally, the majority of respondents to the survey do not plan to introduce new regulations around AI in finance in the near future.

DIGITAL MARKETS

16 September 2024 - Legislative Decree No. 129/2024 adapting national legislation to MiCAR Regulation (EU) 2023/1114 published in the Italian Official Gazette.

Articles 93 and 94 of Regulation (EU) 2023/1114 require Member States to designate the competent authorities (with the necessary supervisory powers) responsible for carrying out the functions and tasks set out therein and to notify the competent authorities (EBA and ESMA) of such designation.

Legislative Decree No. 129 of 5 September 2024 is therefore the national coordinating legislation to the MiCAR Regulation, which fulfils these tasks by identifying the Bank of Italy and CONSOB as the competent national authorities pursuant to Article 93. Among the powers conferred upon them by the legislative decree is also that of issuing provisions implementing the decree (again in accordance with the guidelines adopted by ESMA and the EBA), as well as provisions concerning the manner in which supervisory powers are to be exercised.
Decree 129/2024 then regulates the modalities for the exercise of supervisory and authorisation powers depending on the crypto-activities (asset-linked tokens, or ART, in Chapter II; e-money tokens, or EMT, in Chapter III; crypto-activities other than asset-linked tokens or e-money tokens, in Chapter IV), regulates the authorisation and supervision profiles of crypto-asset service providers, or CASP, in Chapter V, and sets out rules on the prevention and supervision of market abuse.

Finally, the coordinating decree to MiCAR also introduces the first specific national rules on asset-linked tokens and crypto asset service providers and specifies CONSOB's competences and powers regarding the supervision of the obligations of issuers, offerors and persons requesting admission to trading of crypto assets to disclose to the public inside information concerning them.

6 September 2024 - EU Commission: explanatory FAQs for Regulation 2054/2023 (Data Act) released.

The EU Commission has released. an interesting explanatory document in the form of FAQs regarding Regulation 2054/2023 - also known as the Data Act - which will be applicable as of 12 September 2025.

The Data Act establishes a horizontal set of rules on data access and use that respects the protection of fundamental rights and brings wide-ranging benefits to the European economy and society. It increases the availability of data, in particular industrial data, and encourages data-driven innovation, while ensuring fairness in the allocation of the value of data among all actors in the data economy.

The FAQs support the practical implementation of the Data Act and clarify aspects such as: the interaction with other EU regulations (e.g. GDPR, or DMA, etc.), access to and use of data in the context of IoT (Internet of Things), business practices in the context of data sharing; the conditions of access to business data by public authorities in case of emergencies, alternative dispute resolution mechanisms and redress aspects as well as the conditions for switching from one data processing service provider (e.g. cloud) to another, interoperability aspects and future perspectives.

INFORMATION TECHNOLOGY

10 September 2024 - Court of Cassation: electronic serving occurs when the receipt of acceptance is generated.

In a case concerning an application for ineffectiveness of an injunction, the Court of Cassation preliminarily finds that the appeal is inadmissible for lack of proof of service. Specifically, the receipt of acceptance and the receipt of delivery, the so-called RAC, were not deposited in the electronic file nor were they found elsewhere by the clerk of the court.

In its reasoning, the Court reiterates that '*With regard to notification by means of PEC (...) proof of service is constituted by the so-called receipt of delivery (RAC), which constitutes the document capable of proving, until proof to the contrary, that the computer message was received in the addressee's mailbox*'.

This principle was also clarified by the Italian Constitutional Court, which declared the unconstitutionality of Article 16-*septies* of Decree-Law No. 179/2012, insofar as it provides that '*the service performed by telematic means whose acceptance receipt is generated after 9 p.m. and before midnight is perfected for the notifier at 7 a.m. of the following day, instead of at the time of generation of the aforesaid receipt*'.

Therefore, for the purpose of determining the moment of perfection of the telematic notification, neither the moment of sending of the PEC message nor the moment in which the delivery receipt is generated is relevant.

By Order No. 24010 of 6 September 2024, the Supreme Court declared the appeal inadmissible.

CYBERSECURITY

6 September 2024 – National Cybersecurity Agency: the Presidential Decree for the allocation of funds in the three-year period 2024 - 2026 within the National Cyber Security Strategy published.

The DPCM for the allocation of funds for the implementation of the National Cyber Security Strategy 2024-26 was published in the Official Gazette No. 207 of 4 September 2024. Over the three-year period, the measure allocates approximately 347 million euros to the Administrations identified in the Implementation Plan.

The Fund for the Implementation of the National Cybersecurity Strategy and the Fund for Cybersecurity Management were established by Article 1, Section 899 of Law 197/2022. The first Fund serves to finance investments aimed at achieving technological autonomy in the digital sphere and raising the cybersecurity levels of national information systems. The second is intended to support the operational management activities of these projects.

Together with the PNRR funds and the administrations' own resources, they are the main instrument for implementing the National Cybersecurity Strategy 2022 - 2026 and raising the cyber resilience of our country.
