FIVERS

Regulatory update
Data protection, AI, IT and IP

n. 16 / 2024

DATA PROTECTION.

Dec. 10, 2024 - Italian Data Protection Authority: green light for Code of Conduct for management software vendors.

Dec. 4, 2024 - EU Council: reached common position on proposed FiDA (*Financial Data Access*) Regulation to standardize financial data sharing, protect trade secrets, and regulate consent.

Dec. 4, 2024 - The European Data Protection Board (EDPB) adopts a statement on the need for consistency of digital legislation with the GDPR.

ARTIFICIAL INTELLIGENCE.

Dec. 10, 2024 - EuroHPC has selected seven consortia to establish and operate the first artificial intelligence factories across Europe.

December 10, 2024 - Second plenary meeting of the Office for Artificial Intelligence of the EU Commission.

Dec. 8, 2024 - EU Directive 2853/2024 on product liability is in force. New in the area of proof and causation of damage from Artificial Intelligence systems.

DIGITAL MARKETS

December 10, 2024 - The Cyber Resilience Act (CRA) of the European Union is in force.

Dec. 4, 2024 - European Commission: the ViDA (*VAT in the Digital Age)* legislative package on digital VAT is on track.

Dec. 2, 2024 - Published in the Official Journal of the European Union Implementing Regulation (EU) 2024/2956 laying down implementing technical rules for the application of Regulation (EU) 2022/2554 (DORA) regarding standard templates in relation to the register of information of contractual agreements with third-party ICT service providers.

INFORMATION TECHNOLOGY

Dec. 6, 2024 - National Cybersecurity Agency: released video tutorials dedicated to entrepreneurs, employees and suppliers of SMEs to foster better cyber risk awareness.

Dec. 3, 2024 - European Cybersecurity Agency (ENISA): published first ever report on the state of cybersecurity in the EU.

INTELLECTUAL AND INDUSTRIAL PROPERTY

Dec. 8, 2024 - Part of the EU's "*Design Package*," with new updated rules for the legal protection of designs, goes into effect.

DATA PROTECTION

Dec. 10, 2024 - Italian Data Protection Authority: green light for Code of Conduct for management software vendors.

The Italian Data Protection Authority has given the green light to the Code of Conduct of Assosoftware, the Italian Association of Software Manufacturers in Italy, regarding the processing of personal data carried out by management software development and production (SWH) companies.

Such software, intended for companies, associations, professionals and public administration, is used for the fulfillment of tax and social security, welfare and management obligations, the preparation of financial statements, personnel management and corporate obligations, thus having a significant impact on data protection aspects.

In particular, they enable the automation of internal processes of enterprises related to the management of invoicing, customer relations, while for professionals, the management of accounting, tax, labor, and legal activities.

In view of the sensitive nature of the data processed, the Code aims to define a set of rules and technical and organizational measures so that software produced and made available on the market by Assosoftware member companies is developed in compliance with the principles of data protection from the design stage (by design) and by default (by default).

This is to facilitate compliance with the GDPR and to make available to customers suitable tools to fulfill their data protection obligations with regard to processing carried out through software.

In addition to approving the Code of Conduct, the Authority also accredited the related Monitoring Body, composed of experts in the ICT sector, with particular reference to data protection profiles.

Dec. 4, 2024 - EU Council: reached common position on proposed FiDA (Financial Data Access) Regulation to standardize financial data sharing, protect trade secrets, and regulate consent.

The Council of the European Union has reached agreement on the European Commission's June 2023 proposal for a Financial Data Access Framework (FiDA) Regulation.

The FIDA Regulation establishes harmonized rules on the access, sharing, and use of certain categories of data (both personal and non-personal) of customers in financial services. In addition, the FIDA Regulation limits the scope of data sharing to raw data from normal business interactions, excluding confidential business data and trade secrets. It also establishes a data retention limitation period and imposes clear and non-misleading ways of obtaining consent for data sharing from the customer.

Amendments are also introduced to Regulation 2022/1925 (Digital Markets Act - DMA) to prohibit *gatekeepers* from combining service customer data for other purposes and require third-country financial information service providers (FISPs) to appoint a representative established in the EU.

Dec. 4, 2024 - The European Data Protection Board (EDPB) adopts a statement on the need for consistency of digital legislation with the GDPR.

The European Data Protection Board (EDPB) has adopted **a statement on the European Commission's second report on the application of the General Data Protection Regulation (GDPR**), recalling the fundamental importance of legal certainty and consistency of digital legislation-now

extensive and articulated-with the GDPR. With this in mind, the Committee recalls - for example - its ongoing initiatives to clarify the interaction between the application of the GDPR and the AI Act (Regulation 2024/1689), the EU Data Strategy (Regulation 2022/868), and the Digital Services Package (Regulation 2022/2065 - DSA and Regulation 2022/1925 - DMA).

Finally, the EDPB announced that it will intensify content production for non-experts, small and medium-sized enterprises (SMEs) and other groups.

Dec. 4, 2024 - The European Data Protection Board (EDPB) clarifies rules for data sharing with third country authorities and approves certification of the EU data protection seal.

At its latest plenary session, the European Data Protection Board (EDPB) published **guidelines** on **Article 48 of the GDPR** on data transfers to third country authorities and approved a new European data protection seal.

In a highly interconnected world, organizations receive requests from public authorities in other countries to share personal data. Data sharing can, for example, be useful in gathering evidence in case of crime, monitoring financial transactions or approving new drugs.

When a European organization receives a data transfer request from an authority in a "third country" (i.e., non-European countries), it must comply with the General Data Protection Regulation (GDPR). In its guidelines, the EDPB focuses on Article 48 of the GDPR and clarifies how organizations can best assess the conditions under which they can legally respond to such requests. In this way, the guidelines help organizations make a decision about whether they can legally transfer personal data to third country authorities when requested.

Judgments or decisions of third country authorities cannot be automatically recognized or enforced in Europe. If an organization responds to a request for personal data from an authority in a third country, this data flow constitutes a transfer and the GDPR applies. An international agreement may provide both a legal basis and a ground for transfer. Where no international agreement exists or where the agreement does not provide an adequate legal basis or safeguards, other legal bases or other grounds for transfer could be considered in exceptional circumstances and on a case-by-case basis.

The guidelines are subject to public consultation until January 27, 2025.

At the plenary meeting, the Board also adopted an opinion approving the *Brand Compliance* certification criteria related to processing activities by controllers or processors. In September 2023, the Board had already adopted an opinion on approving national *Brand Compliance* certification criteria. The approval of the new opinion means that these criteria will now be applicable throughout Europe and as a European seal for data protection.

GDPR certification helps organizations demonstrate their compliance with the Data Protection Act.

ARTIFICIAL INTELLIGENCE.

Dec. 10, 2024 - EuroHPC has selected seven consortia to establish and operate the first artificial intelligence factories across Europe.

The European High Performance Computing Joint Undertaking (EuroHPC) has selected seven proposals to establish and operate the first AI factories across Europe. This is a milestone for Europe in building an ecosystem to train advanced AI models and develop AI solutions.
With an investment of 1.5 billion euros, the selected artificial intelligence factories involve 15 member states r will be housed at major research and technology hubs across Europe, precisely in the following cities:

Barcelona, Spain: "BSC AIF" at the Barcelona Supercomputing Center
Bologna, Italy: "IT4LIA" at CINECA - Bologna Tecnopolo
Kajaani, Finland: "LUMI AIF" and CSC
Bissen, Luxembourg: "Meluxina-AI" and LuxProvide
Linköping, Sweden: "MIMER" at Linköping University.
Stuttgart, Germany: "HammerHAI" at the University of Stuttgart.
Athens, Greece: "Pharos" at GRNET

The seven AI factories involve 15 member states and two EuroHPC participating states. Portugal, Romania, and Turkey have joined the BSC AIF; Austria and Slovenia have joined ITA4LIA; and Czechia, Denmark, Estonia, Norway, and Poland have joined the AIF UMI.

New supercomputers optimized for artificial intelligence will be developed at five of the selected sites (Finland, Germany, Italy, Luxembourg, and Sweden). The artificial intelligence factories in Spain and Finland will also be equipped with an experimental platform, which will provide a state-of-the-art infrastructure for the development and testing of innovative artificial intelligence models and applications.

Artificial intelligence factories will double the computing capacity of EuroHPC, meeting specific needs and enhancing European capabilities in artificial intelligence.

December 10, 2024 - Second plenary meeting of the Office for Artificial Intelligence of the EU Commission.

The AI Office is a body created by EU Regulation 2024/1689 *(AI Act)* and has the specific function of supporting the EU Commission. Relevant topics were addressed in its second plenary session, including:

- Austria and Norway's 'AI literacy' initiatives;
- national measures on AI *governance* introduced by Malta, Finland and Slovenia;
- The strategic vision for AI of the new EU Commission;
- updates on international activities, including (a) collaboration between the European Union and Singapore; (b) presentation of the report on the outcomes of the OECD Ministerial Summit on the Global Partnership on AI; and (c) presentation of the risk management framework that the Council of Europe's Committee on AI recently adopted;
- Update on the status of work on the adoption of the code of practice for AI for general use;
- Discussion on guidelines for prohibited AI practices and system definitions;
- action plan for 2025.

Dec. 8, 2024 - EU Directive 2853/2024 on product liability comes into force. New in the area of proof and causation of damage from Artificial Intelligence systems.

On December 8, 2024, the Directive of the European Parliament and of the Council on Liability for Defective Products and Repealing Council Directive 85/374/EEC (Product Liability Directive) came into force.

The Directive is especially important because it updates liability rules to the digital age and introduces provisions on Artificial Intelligence Liability.

Illuminating is the provision of Recital 13 of the Directive:

(13) Products in the digital age can be tangible or intangible. Software, such as operating systems, firmware, computer programs, applications, or AI systems, is increasingly prevalent in the market,

and its importance for product security purposes is growing. Software can be placed on the market as a stand-alone product or can later be integrated into other products as a component and can cause damage due to its operation. To ensure legal certainty, it should be clarified in this directive that, for the purposes of applying strict liability, software is a product, regardless of how it is supplied or used, and thus regardless of whether the software is integrated into a device, used through a communications network or cloud technologies, or is provided through a software-as-a-service model. Information, on the other hand, should not be considered a product, and product liability rules should therefore not apply to the content of digital files, such as multimedia files, e-books, or the mere source code of software. The manufacturer or developer of software, including the provider of IA systems under Regulation (EU) 2024/1689 of the European Parliament and of the Council (5), should be considered a manufacturer.

So, a developer or producer of software, including artificial intelligence (AI) systems within the meaning of Regulation 2024/1689 (AI Act) are considered "manufacturers," as best understood from Article 4(10) of the directive:

"Manufacturer" means *any natural or legal person who: (a) develops, produces or manufactures a product; (b) has a product designed or manufactured or who, by affixing its name, trademark or other distinguishing features to such product, presents itself as a manufacturer; or (c) develops, produces or manufactures a product for its own use.*

The Product Liability Directive also states that since products can be designed in such a way that software changes, including upgrades, can be made, the same principles apply to the changes made. Accordingly, when a substantial modification is made by a software update or an update due to the continuous learning of an AI system, the substantially modified product is considered to have been made available on the market or put into service at the time of the modification.

Fundamental are the procedural rules regarding proof of damage and causation, proof that is often almost impossible to be provided by the injured party, especially in the case of damage created by AI systems, due to the so-called "black box" effect of the algorithm.

They may therefore presume the defective character of a product or the causal link between damage and defect, or both, in cases where, although the defendant manufacturer has disclosed the relevant information, it is excessively difficult for the injured party-actor, particularly because of the technical and scientific complexity of the case, to prove the defective character of the product or the existence of the causal link, or both. Accordingly, peer not jeopardize the right to compensation and given that manufacturers have specialized knowledge and better information than the injured party, and in order to ensure a fair allocation of risks by avoiding reversal of the burden of proof, where his difficulties concern proof of the defective character of the product the plaintiff will be required to prove only that it is probable that the product was defective or, where his difficulties concern proof of causation, only that the defective character of the product is a probable cause of the damage. Technical or scientific complexity will be determined by the national courts on a case-by-case basis, taking into account several factors: from the complex nature of the product, as in the case of an innovative medical device to the complex nature of the technology used, e.g., machine learning; from the complex nature of the information and data that the plaintiff must analyze to the complex nature of the causal link, e.g., between a pharmaceutical or food product and the occurrence of a disease, or a link for whose proof the plaintiff is required to explain the inner workings of an AI system. The plaintiff will have to provide arguments to prove the existence of the above-mentioned undue hardship, but will not be required to provide evidence regarding such hardship. For example, in an action involving an AI system, in order for the court to establish the existence of undue hardship, the plaintiff will not be required to explain the specific features of that AI system or how those features complicate the proof of causation. The defendant - instead - will still have the opportunity to challenge all elements of the action, including the existence of undue hardship.

DIGITAL MARKETS

December 10, 2024 - The Cyber Resilience Act (CRA) of the European Union is in force.

On December 10, 2024, the *Cyber Resilience Act* (EU Regulation 2024/2847 on horizontal cybersecurity requirements for products with digital elements) came into force, which introduced mandatory cybersecurity requirements for hardware and software products with digital elements.

The Regulations will be applicable as of December 11, 2027, with the exception of producer reporting requirements, which will apply as of September 11, 2026.

The new regulations stipulate that products with digital elements must meet several requirements to ensure their cybersecurity and to be placed on the market, including:

- Security requirements related to the properties of such products, including that product design, development, and production be carried out in such a way as to ensure an adequate level of cybersecurity, with a risk-based approach; and
- vulnerability management requirements, such as identifying and documenting vulnerabilities and implementing tests, policies and measures to facilitate information sharing.

In addition, the CRA clarifies-in Article 7-what *products* qualify as "*products with important digital elements*" and what additional requirements must be met. There are also specific coordination and harmonization provisions with Regulation 2024/1689 on artificial intelligence for high-risk artificial intelligence (AI) systems.

The law clarifies the obligations imposed on producers, which include:

- ensure compliance with the essential requirements for their products when they are placed on the market, in particular by conducting conformity assessments;
- Conduct a cybersecurity risk assessment and include it in the technical documentation;
- Perform specific *due diligence* on components from third parties;
- Implement appropriate policies and procedures, including coordinated vulnerability disclosure policies;
- Ensure that products remain in compliance and take corrective action in case of misalignment from compliance; and
- Provide users with complete information and instructions.

The manufacturer must, without undue delay and in any case within 24 hours of becoming aware of it, notify the *Computer Security Incident Response Team* (CSIRT) and the European Union Cybersecurity Agency (ENISA) of any vulnerability actively exploited with respect to the product with digital elements, also notifying any security impact to users. The incident notification must be sent within 72 hours of becoming aware of the incident. The CRA also allows for voluntary notification of any vulnerabilities or cyber threats that could affect a product's risk profile. ENISA is mandated to establish a single communication platform.

With regard to users, manufacturers must inform them, without undue delay and after becoming aware of the incident, about any incident and, if necessary, about the corrective measures that users can implement to mitigate the impact of the incident.

Anticipated penalties can be up to 15 million euros or, for companies, up to 2.5 percent of the previous year's total annual worldwide turnover, whichever is higher.

Dec. 4, 2024 - European Commission: the ViDA (*VAT in the Digital Age)* legislative package on digital VAT is on track.

By adopting and promoting digitization, the ViDA package makes the EU VAT system more business-friendly and more resilient to fraud. The new rules also mark the first step in addressing the challenges arising from the platform economy and helps create a level playing field between short-term accommodation services and online and traditional transportation services.

The package introduces 3 measures:

1. The new system introduces uniform real-time digital reporting for VAT purposes based on e-invoicing for cross-border transactions, which will provide Member States with the valuable information they need in a timely manner to step up the fight against VAT fraud. E-invoicing will further accelerate the transformation of businesses into the digital age by simplifying transactions, ensuring compliance and security, enabling data-driven decision-making, and supporting scalability for future growth and innovation.

2. Platform economy operators in the passenger transport and short-term accommodation services sector will also become responsible for collecting VAT and paying tax to tax authorities if the indirect supplier does not charge VAT. The measure will help improve the level playing field between online and traditional services and facilitate activities for indirect operators who will not be responsible for VAT.

3. Finally, the initiative will reduce the need to register multiple times in different member states through the expansion of the existing "one-stop-shop" VAT model already in place for business enterprises.

Dec. 2, 2024 - Published in the Official Journal of the European Union Implementing Regulation (EU) 2024/2956 laying down implementing technical rules for the application of Regulation (EU) 2022/2554 (DORA) regarding standard templates in relation to the register of information of contractual agreements with third-party ICT service providers.

The EU Commission's Implementing Regulation (EU) 2024/2956-applicable as of December 22, 2024-introduces the standard templates in relation to the register of information on contracts with third-party information and communication technology (ICT) service providers.

Article 28(3) of the DORA Regulation requires financial entities to maintain a detailed register of all contractual arrangements with third-party ICT service providers that fall within the scope of management of emerging risks represented by specific ICT service providers supporting business processes and financial services rendered by financial entities (banks, insurance companies, brokers, etc.). This register should include specific information about the contracts, such as duration, services provided, and security measures taken.

The implementing regulation therefore introduces standard templates for recording information, ensuring uniformity and consistency in data collection and management. These templates help facilitate supervision and management of cyber risks represented by third-party ICT service providers. The information collected in the registry is essential for the internal management of financial entities' cyber risks and for effective supervision by competent authorities. ESAs (EBA, EIOPA, ESMA) will use this information for their inspection and monitoring tasks and to designate *critical* third-party ICT service providers, a designation that will be precisely based on the information collected in the registries by financial entities.

To reduce administrative costs, financial groups may maintain a single register of information on a sub-consolidated and consolidated basis, as long as each financial entity is allowed to fulfill its obligations to maintain and update information.

INFORMATION TECHNOLOGY

Dec. 6, 2024 - National Cybersecurity Agency (NCA): released video tutorials dedicated to entrepreneurs, employees and suppliers of SMEs to foster better cyber risk awareness.

ACN has produced three video tutorials to foster better cyber risk awareness. The tutorials target three distinct categories of users: business owners, executives and employees, and focus on enhancing cybersecurity in strategic business planning. They also provide tips for increasing employee awareness; helping consultants and vendors interface securely and effectively with small and medium-sized businesses.

The tutorials were expressly designed as an element of the campaign "*Let's Ignite Cybersecurity. Let's Protect Our Businesses*" dedicated to small and medium-sized enterprises (SMEs) and aim to inform business operators and their customers of the importance of being prepared to deal with cyber risks, reducing exposure to cyber threats and mitigating the impacts of any cyber attacks.

The campaign implements measure #71 of the National Cybersecurity Strategy 2022 - 2026 on "*Promoting Cybersecurity Culture*" Reference links are provided below: (i) ACN's tips for SMEs (ii) campaign video tutorial "Let's Access Cybersecurity. Let's protect our businesses."

Dec. 3, 2024 - European Cybersecurity Agency (ENISA): published first ever report on the state of cybersecurity in the EU.

Pursuant to Article 18 of the NIS 2 Directive, ENISA released the first biennial report on the state of cybersecurity in the European Union.

The report provides an evidence-based overview of the state of European cybersecurity and an assessment of cybersecurity capabilities across Europe. The report also contains policy recommendations to address the identified gaps and increase the level of cybersecurity in the EU.

The report identifies four priority areas: 1) policy implementation, 2) cyber crisis management, 3) supply chain, and 4) skills, and within this framework provides six policy recommendations:

- Strengthen the technical and financial support provided to EU institutions, bodies, and agencies (EU institutions, bodies, and organs) and relevant national authorities and entities within the scope of the NIS 2 Directive to **ensure harmonized, comprehensive, timely, and consistent implementation of the evolving EU cybersecurity policy framework** using existing EU-level structures such as the NIS Cooperation Group; Network of CSIRTs and EU Agencies.
- As requested by the Council, **revise the EU plan for a coordinated response to large-scale cyber incidents,** taking into account all the latest developments in EU cybersecurity policy. The revised EU plan should **further promote the harmonization and optimization of EU cybersecurity, as well as strengthen both national and EU cybersecurity capabilities** to increase cybersecurity resilience at national and European levels.
- **Strengthen the EU cyber workforce** through the implementation **of the Cybersecurity Skills Academy** and in particular by defining a **common EU approach to cybersecurity training**, identifying future skills needs, developing a **coordinated EU approach to**

stakeholder engagement to close the **skills gap in skills**, and establishing a **European cybersecurity skills attestation system.**

- Address supply chain security in the EU **by intensifying coordinated EU-wide risk assessments** and **the development of a horizontal EU strategic framework for supply chain security** to address cybersecurity challenges faced by both the public and private sectors.
- **Improve understanding of sector specificities and needs, improve the level of cybersecurity maturity of sectors covered by the NIS2 directive, and use the future cybersecurity contingency mechanism to be established under the Cybersecurity Solidarity Act** for sector preparedness and resilience, with a focus on weak or sensitive sectors and risks identified through EU-wide risk assessments.
- Promote a **unified approach** by building on existing policy initiatives and harmonizing national efforts to achieve a **high common level of cyber security and cyber hygiene awareness among professionals and citizens,** regardless of demographic characteristics.

INTELLECTUAL AND INDUSTRIAL PROPERTY

Dec. 8, 2024 - Part of the EU's "*Design Package*," with new updated rules for the legal protection of designs, goes into effect.

The two pieces of legislation in the so-called "Design package" with which the EU Commission aimed to update and modernize existing rules (to address challenges from emerging technologies such as 3D printing, metaverse and artificial intelligence), as well as make design protection more appropriate for new products, entered into force on Dec. 8, 2024.

The Design Package consists of:

- Of Directive (EU) 2024/2823 of October 23, 2024 on the legal protection of designs

- Of Regulation (EU) 2024/2822 amending Regulation (EC) No. 6/2002 on Community Designs and repealing Regulation (EC) No. 2246/2002.

The new European Design Regulation will be applicable as of May 1, 2025, while provisions requiring additional laws will take effect as of July 1, 2026.

The Design Directive will enter into force on December 8, 2024, but member states will have until December 9, 2027, to adapt their national legislation (in Italy's case: the Industrial Property Code).
