FIVERS

Update
Data protection, AI, IT and IP

No. 4 / 2025

DATA PROTECTION.

7 February 2024 – AI and GDPR: the CNIL publishes new recommendations on how to render privacy policies and how to manage the instances of exercising*data protection rights* with respect to the specificities of Artificial Intelligence systems and models.

ARTIFICIAL INTELLIGENCE.

18 February 2025 – Agency for Digital Italy (AgID): Guidelines for the adoption of Artificial Intelligence in the Public Administration have been published.

---

12 February 2025 – European Insurance Authority: the Opinion on the application of the Artificial Intelligence Regulation to the insurance sector is in public consultation.

---

7 February 2025 – EU Commission: published the Guidelines on the interpretation of the legal concept of "artificial intelligence system" pursuant to Article 3(1) of Regulation 2024/1689 (AI Act).

CYBERSECURITY

18 February 2025 – Bank of Italy: operating instructions and format for the ICT DORA self-assessment.

---

18 February 2025 – DORA European Supervisory Authorities: updated the FAQ on the compilation and keeping of information registers.

---

14 February 2025 – IVASS: letter to the market on the operating procedures for the notification of major ICT incidents under the DORA Regulation.

---

13 February 2025 – EU Commission: published the regulatory technical standards (RTS) implementing the DORA obligations on the implementation of the Test-led-penetration-test – TLPT.

---

12 February 2025 - In the Official Gazette the Prime Ministerial Decree of 9 December 2024, no. 221 containing the criteria for the application of the safeguard clause referred to in the Legislative Decree transposing the NIS 2 Directive.

---

7 February 2025 – The National Agency for Cybersecurity (ACN) reminds all NIS subjects of the deadline of 28 February to register.

---

5 February 2025 – ENISA: The EU Cybersecurity Agency publishes the 2025-2027 work programme.

---

4 February 2025 – European Union: Regulation 2025/35 (*Cyber Solidarity Act*) entered into force.

DIGITAL MARKETS

13 February 2025 – European Parliament: green light for the regulatory package on digital VAT.

DATA PROTECTION

7 February 2024 – AI and GDPR: the CNIL publishes new recommendations on how to render privacy policies and how to manage the instances of exercising*data protection rights* with respect to the specificities of Artificial Intelligence systems and models.

The GDPR enables the development of innovative and responsible AI in Europe. The new recommendations of the CNIL illustrate this by providing concrete solutions to inform the people whose data is used and to facilitate the exercise of their rights.

Adapt GDPR principles to the specificities of AI.

Some AI models are anonymous and therefore not subject to the GDPR. However, other models, such as a large language model (LLM), may contain personal data. The European Data Protection Board (EDPB) recently provided relevant criteria on the application of the GDPR to AI models.

When applying the GDPR, people's data must be protected, either within training datasets, within models that may have stored data, or through the use of the model via prompts. While the fundamental principles of data protection remain applicable, they need to be adapted to the specific context of AI.

The CNIL has long established that:

- Purpose determination should be applied flexibly to general-purpose AI systems: an operator who is unable to define all potential applications in the training phase can instead describe the type of system under development and illustrate the main potential functionalities.
- The principle of data minimization does not prevent the use of large training datasets. However, data should generally be sorted and cleaned to optimize algorithm training, while avoiding unnecessary processing of personal data.
- The retention of training data may be extended if justified and if the dataset is subject to appropriate security measures. This is particularly important for databases that require significant scientific and financial investment, which sometimes become recognized standards within the research community.
- In many cases, the re-use of databases, including those available online, is possible, provided that the data has not been unlawfully collected and that their re-use is in line with the original purpose of the collection.

The two new Recommendations: IA and Information to Data Subjects and AI and Exercise of Data Protection Rights.

The CNIL has published two new Recommendations to promote the responsible use of AI, while ensuring compliance with the protection of personal data. These recommendations confirm that the requirements of the GDPR are sufficiently balanced to address the specific challenges of AI. They provide concrete and proportionate solutions to informpeople and facilitate the exercise of their rights.

When personal data is used to train an AI model and can potentially be stored by it, the data subjects must be informed.

The way this information is provided can be tailored based on risks to individuals and operational constraints. Under the GDPR, in some cases, especially when AI models rely on third-party data sources and the provider cannot contact individuals directly, organizations may limit themselves to general information (e.g., published on their website). When multiple sources are used, as is common with general-purpose AI models, broad disclosure indicating source categories or listing a few key sources is usually sufficient.

As for the Recommendation on the exercise of rights, European legislation gives individuals the right to access, rectify, oppose and delete their personal data.

However, exercising these rights can be particularly challenging in the context of AI models, both because

of the difficulties in identifying individuals within the model and because of the modification of the model itself. The CNIL urges AI developers to embed privacy protection from the design stage, to pay special attention to personal data within training datasets, to strive to anonymize models whenever this does not compromise the intended purpose, and to develop innovative solutions to prevent the disclosure of confidential personal data by AI models.

In some cases, cost, technical impossibility or practical difficulties may justify refusing to comply with a request to exercise these rights. However, where the right is to be guaranteed, the CNIL will consider reasonable accommodations available to the creator of the model and may authorise flexible deadlines for responding to applications. The CNIL also points out that scientific research in this area is evolving rapidly and urges AI stakeholders to stay informed about the latest advances to ensure the best possible protection of people's rights.

ARTIFICIAL INTELLIGENCE.

18 February 2025 – Agency for Digital Italy (AgID): Guidelines for the adoption of Artificial Intelligence in the Public Administration have been published.

From 18 February to 20 March 2025, the Guidelines for the adoption of Artificial Intelligence in the Public Administration, adopted with Determination no. 17/2025, are in public consultation.

Envisaged by the Three-Year Plan for Information Technology in the Public Administration 2024-2026, the AgID Guidelines for the adoption, purchase and development of AI systems in the Public Administration are issued following the procedure provided for in Article 71 of the Digital Administration Code (CAD). Those under consultation concern, specifically, the methods of adopting Artificial Intelligence systems, with particular reference to the aspects of regulatory compliance and organizational impact.

It is possible to participate in the consultation, providing comments and suggestions, through the Forum Italia platform

---

12 February 2025 – European Insurance Authority (EIOPA): the Opinion on the application of the Artificial Intelligence Regulation to the insurance sector is in public consultation.

The European Insurance and Occupational Pensions Authority (EIOPA) has put its *Opinion on the governance and risk management of artificial intelligence for public consultation*, which provides guidance to supervisors and insurance undertakings on how to interpret and implement the provisions of the insurance sector in light of the use of AI systems in the insurance sector.

EIOPA's opinion provides further clarity on the fundamental principles and requirements provided for in insurance industry legislation that should be taken into account in relation to the use of AI systems.

It applies to those AI systems that are not considered prohibited or high-risk AI practices under the AI Act.

While insurance legislation applies to all AI systems used in the insurance sector, to avoid regulatory complexity and overlap, the scope of the opinion does not cover prohibited AI practices or high-risk AI systems under the AI Act. It is based on the principle of proportionality and follows a principled approach, ensuring that it is flexible enough to adapt to technological and market developments over time.
The opinion is in line with the basic principles and requirements of the AI Act and other international initiatives in this area, such as those of the Organisation for Economic Co-operation and Development (OECD), the G20 or the International Association of Insurance Supervisors (IAIS), thereby supporting a harmonised approach.

The opinion sets out high-level supervisory expectations regarding the governance and risk management principles that insurance undertakings should apply to ensure responsible use of AI systems adapted to specific use cases. These principles, among others, include:

- apply a proportionate and risk-based approach throughout the life cycle of AI systems,
- act on the basis of fairness and ethical principles, in the best interests of consumers,
- clearly define the roles and responsibilities of the staff concerned,
- be able to meaningfully explain the results of AI systems,
- the implementation of robust data governance policies and
- maintain adequate and orderly documentation and records.

---

7 February 2025 – EU Commission: published the Guidelines on the interpretation of the legal concept of "artificial intelligence system" pursuant to Article 3(1) of Regulation 2024/1689 (AI Act).

The interpretative action of the AI Act carried out by the EU Commission continues. After the recent approval of the Guidelines on prohibited AI practices, here is the adoption of the interpretative guidelines on the legal definition of "artificial intelligence system" (art. 3.1 Reg. 1689/2024).

These Guidelines, like those on prohibited practices, are currently approved but not yet formally adopted. These are relevant acts (although not binding) since – as mentioned in previous posts – the direct applicability as of 2 February 2025 of the first 5 articles (including Article 3, which contains 68 legal definitions) now allows not only to review contracts with providers of AI-based services and products from this perspective, but also (and this is what the latest guidelines aim at) to assist suppliers and other interested parties in the determine whether a software system constitutes an "AI system" and is therefore subject to the rules of the Regulation.

To be covered by the AI Act, we need to look at (a) the architecture of the system, (b) the specific functionalities, and (c) the presence of the seven elements mentioned in the definition in Article 3(1) of the AI Act, namely:

1. Machine-based system;
2. Autonomy;
3. Adaptability;
4. Pursuit of implicit or explicit objectives;
5. Inference and output generation using AI techniques;
6. Outputs such as forecasts, content, recommendations or decisions;
7. Outputs that may affect physical or virtual environments.

CYBERSECURITY

18 February 2025 – Bank of Italy: operating instructions and format for the ICT DORA self-assessment.

With the Communication to the market of 23 December 2024 on ICT security, financial entities were invited by the Bank of Italy to assess their positioning with respect to the requirements introduced by EU Regulation 2022/2554 on Digital Operational Resilience (DORA) and to carry out a self-assessment of their ICT risk management system.

To facilitate financial entities in conducting the required analyses and, at the same time, to promote the comparability of responses, the Bank of Italy has made available to intermediaries

- Operating instructions relating to the assessments required by the Communication to the market on ICT security
- ICT risk self-assessment template

---

18 February 2025 – DORA European Supervisory Authorities: updated the FAQ on the compilation and keeping of information registers.

The European Supervisory Authorities (ESAs) have updated the FAQs on the reporting of information registers under Article 28(3) of the DORA Regulation. The update includes details on what information needs to be reported from 2025 onwards, how to maintain and report records at various levels, and reporting deadlines for 2025 and 2026. Other aspects clarified in the FAQs concern technical profiles such as the format required for registers, the use of templates and file naming conventions for reporting to the ESAs.

---

14 February 2025 – IVASS: letter to the market on the operating procedures for the notification of major ICT incidents under the DORA Regulation.

IVASS has announced the operating procedures by which insurance companies and larger insurance, reinsurance and ancillary insurance intermediaries are required to promptly send the Institute reports of serious cyber incidents and, on a voluntary basis, cyber threats pursuant to the European DORA Regulation (EU Reg. 2022/2554 - Digital Operational Resilience Act).
The DORA Regulation, applicable from 17 January 2025, aims to achieve the adequate resilience of operators and the European financial system, identifying, among other things, measures for the prevention, response and resumption of operations in the event of an attack or incident.

---

13 February 2025 – EU Commission: published the regulatory technical standards (RTS) implementing the DORA obligations on the implementation of the Test-led-penetration-test – TLPT.

The European Commission has published the Technical Regulatory Standard (RTS) for the implementation of *Threat-Led Penetration Testing (TLPT)* pursuant to the DORA Regulation.

Only financial entities that have a certain degree of systemic importance and are sufficiently ICT-mature are required to carry out a TLPT.

The financial entities required to carry out a TLPT will be determined by the TLPT authorities. The TLPT authorities are defined in Article 1(7) of the RTS and include the public authority for the financial sector of the EU Member State. When determining the financial entities required to conduct a TLPT, the TLPT Authority may consider, inter alia:

- systemic and impact factors, such as:
  - the size of a financial entity and whether it provides financial services in more than one EU Member State;
  - the criticality or importance of the services provided;
  - the substitutability of the services provided; and
  - the complexity of the business model; and
- ICT-related risk factors, including:
  - the risk profile;
  - the threat landscape;
  - the degree of dependence on essential or important functions of the financial entity; and
  - the maturity of operational ICT security detection and mitigation measures.

---

12 February 2025 - In the Official Gazette the Prime Ministerial Decree of 9 December 2024, no. 221 containing the criteria for the application of the safeguard clause referred to in the Legislative Decree transposing the NIS 2 Directive.

The Prime Ministerial Decree no. 221 of 9 December 2024 was published in the Official Gazette no. 33 of 10 February 2025, which defines the criteria for the application of the safeguard clause provided for by art. 3, paragraphs 4 and 12, of Legislative Decree no. 138/2024.

The measure is part of the transposition of Directive (EU) 2022/2555 (NIS 2 Directive), aimed at strengthening cybersecurity at European level, and provides operational guidance for the exclusion of certain companies from the application of the cybersecurity measures provided for by the NIS decree.

The regulation, adopted on the proposal of the National Cybersecurity Agency, establishes clear criteria for derogation from the rules on the security of network and information systems, introducing a registration and evaluation mechanism for applicants. The aim is to ensure a balance between cybersecurity protection and the proportionality of the measures imposed on companies, avoiding disproportionate burdens for companies that operate with infrastructural and managerial autonomy.

The criteria for the application of the safeguard clause referred to in art. 3 of the Prime Ministerial Decree:

1. The request for the application of the safeguard clause may be granted if the entity jointly declares:

(a) the total independence of its NIS information and network systems from those of the associated undertakings, in the sense that the information and network systems of the associated undertakings do not contribute in any way to the functioning of the NIS information and network systems of that entity;

b) the total independence of its NIS activities and services from those of the associated companies, in the sense that the activities and services of the associated companies do not contribute in any way to the performance of the activities and the provision of the NIS services of the same entity.

2. The safeguard clause may not be requested by the person to whom the provisions of the NIS decree apply pursuant to Article 3, paragraph 10, of the same decree.

---

7 February 2025 – The National Agency for Cybersecurity (ACN) reminds all NIS subjects of the deadline of 28 February to register.

The new NIS (Network and Information Security) directive, implemented in Italy with Legislative Decree 138/2024, has now entered into force on 16 October 2024. The Directive aims to strengthen the security of networks and information systems, based on legislation that introduces deadlines and specific obligations for public and private organisations operating in essential sectors.

For all NIS subjects, from December 1 to February 28 it is possible to register through the National Cybersecurity Agency's services portal.

In order to ensure smooth registration, ACN recommends that you immediately register your contact point and complete the declaration on the service portal.

In the section dedicated to the new NIS discipline there is information material and a large collection of answers to frequently asked questions that are constantly updated. ACN points out, in particular, FAQ 3.1 which outlines the self-assessment process that potential NIS subjects will have to carry out to determine the need, or not, to register.

Finally, ACN reminds that the last deadline for registration, for all NIS subjects, will expire on 28 February and that failure to register by the aforementioned date is assisted by the administrative fines provided for by Article 38, paragraphs 10 and 11, of the NIS decree, up to a maximum of 0.1% of turnover.

---

5 February 2025 – ENISA: The EU Cybersecurity Agency publishes the 2025-2027 work programme.

On 5 February 2025, the European Union Agency for Cybersecurity (ENISA) published a single programming document outlining the 2025-2027 multiannual programming and the work programme for 2025.

The programme details ENISA's objectives and activities, including the establishment of an EU vulnerability database and a register for digital entities to improve cross-border collaboration, as well as reporting on the state of EU cybersecurity.

The overall programme covers, inter alia, ENISA's operational and business objectives and activities in relation to the transposition of the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), as well as the impact of the Cyber Resilience Act (CRA), the Cyber Solidarity Act (CSA) and the Digital Operational Resilience Act (DORA).

---

4 February 2025 – European Union: Regulation 2025/35 (Cyber Solidarity Act) entered into force.

On 4 February 2025, Regulation 2025/35 establishing measures to strengthen the Union's solidarity, threat and cyber incident detection, preparedness and response capabilities, and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) entered into force and is applicable 25 25 was officially published in the Official Journal of the European Union, and amending Regulation (EU) 2021/694 (Cyber Solidarity Act).

The new regulation sets out the EU's capabilities to make Europe more resilient and responsive to cyber threats, while strengthening cooperation mechanisms.

It is mainly aimed at:

- support the detection and awareness of significant or large-scale cybersecurity threats and incidents
- strengthen preparedness and protect critical entities and essential services, such as hospitals and public services
- strengthen solidarity at EU level, concerted crisis management and response capacities in all Member States
- help ensure a secure digital landscape for citizens and businesses

To detect serious cyber threats quickly and effectively, the new regulation establishes a '*cybersecurity alert system*', i.e. a pan-European infrastructure consisting of national and cross-border IT hubs across the EU. These are responsible for sharing information and detecting and acting on cyber threats. They will strengthen the existing European framework while, in turn, the relevant authorities and actors will be able to respond more efficiently and effectively to major incidents.

The new regulation also provides for the creation of a cybersecurity emergency mechanism to increase preparedness and enhance incident response capabilities in the EU. This mechanism will support:

- preparedness actions, including carrying out audits of entities operating in highly critical sectors (health, transport, energy, etc.) to detect potential vulnerabilities based on common risk scenarios and methodologies
- A new EU cybersecurity reserve, consisting of private-sector incident response services that are ready to intervene at the request of a Member State or EU institutions, bodies, offices and agencies, as well as associated third countries, in the event of significant or large-scale cybersecurity incidents
- mutual assistance in financial terms

Finally, the new Regulation establishes an evaluation and review mechanism to assess, inter alia, the effectiveness of actions under the Cybersecurity Emergency Mechanism and the use of the cybersecurity reserve, as well as the contribution of the Regulation to strengthening the competitive position of the industrial and services sector.

Targeted amendment of the 2019 Cybersecurity Act.

The targeted amendment aims to strengthen the EU's cyber resilience by enabling the future adoption of European certification schemes for 'managed security services'. Managed security services, offered to customers by specialised companies, are essential for the prevention, detection, response to or recovery from cybersecurity incidents. They may consist, for example, of incident management, penetration testing, security audits and technical assistance consultancy.

The amendment will allow the introduction of European certification systems for managed security services. It will help to increase their quality and comparability, promote the emergence of reliable cybersecurity service providers and avoid fragmentation of the internal market, as some Member States have already started to adopt national certification schemes for managed security services. Pending the regular review of the Cybersecurity Act, expected by 28 June 2024, the provisional agreement:

- clarifies the definition of 'managed security services' and ensures alignment with the revised Network and Information Systems Directive (NIS 2)
- aligns the security objectives of those certification schemes with the security objectives of other schemes under the existing Cybersecurity Act
- contains amendments to the Annex to the Cybersecurity Act, which includes a list of requirements to be met by conformity assessment bodies
- specifies that ENISA should consult all relevant stakeholders in a timely manner and provides for the possibility for ENISA or the Commission to submit quarterly briefings to the co-legislators on the functioning of the certification schemes.

DIGITAL MARKETS

13 February 2025 – European Parliament: green light for the regulatory package on digital VAT.

After approval by the EU Council on 24 November 2024, the European Parliament has given the green light to update the VAT legislation with the aim of adapting it to the dynamics of the digital market. The adoption of the amendments, which incorporate the indications expressed by the Member States last November, represents a significant step in the fight against distortions of competition and tax fraud.

VAT obligation for digital platforms

One of the most relevant aspects of the reform concerns the introduction of the obligation to pay VAT for services provided through online platforms. From 2030, these platforms will be required to collect and remit the tax in most cases where individual service providers do not do so themselves. The measure aims to put an end to a regulatory disparity that has so far favoured some sectors of the digital economy, such as short-term rentals and road passenger transport, compared to traditional economic activities, which are already subject to VAT.

Member States will still be able to provide exemptions for small and medium-sized enterprises, in line with the position expressed by the European Parliament, in order to mitigate the bureaucratic impact for small companies.

Digitization of VAT returns and fight against fraud

A further pillar of the reform is the digitalisation of VAT reporting obligations for cross-border transactions. By 2030, businesses will be required to issue e-invoices for international business-to-business (B2B) transactions, with automated reporting of data to the relevant tax authorities. This innovation will strengthen the fight against VAT fraud, allowing supervisory bodies to monitor transactions in real time and reduce the so-called "VAT gap", i.e. the difference between the taxes actually collected and those due.

Administrative simplification: strengthening the one-stop shops

To reduce the administrative burden on businesses operating internationally, the legislation provides for the enhancement of online VAT one-stop shops. Thanks to this measure, an increasing number of companies will be able to comply with their tax obligations through a single portal and in a single language, promoting greater uniformity and simplification in the VAT collection system at EU level.

Economic impact and future prospects

The update of the VAT rules is the result of a review process that lasted over two years and is part of the broader regulatory package "VAT in the digital age" (ViDA), presented by the European Commission on 8 December 2022. The Commission estimates that adopting these measures will allow Member States to recover up to €11 billion of uncollected VAT each year for the next decade. In addition, businesses will benefit from an estimated €4.1 billion in annual savings in compliance costs and €8.7 billion in administrative and registration costs.

With this reform, the European Union takes a decisive step towards a fairer, more transparent tax system adapted to the needs of the digital market, ensuring greater efficiency for both companies and national tax administrations.
