FIVERS

Regulatory update
Data protection, AI, IT and IP

n. 4 / 2024

DATA PROTECTION

17 June 2024 - Italian Data Protection Authority: published the final guideline on the processing and storage of e-mail metadata of public and private workers.

---

13 June 2024 – EU: Multistakeholder Expert Group to Commission publishes evaluation of the GDPR.

---

12 June 2024 - Italian Data Protection Authority: favourable opinion on the draft Regulation for PA digital infrastructures and cloud services prepared by the Agency for National Cybersecurity (ACN).

---

12 June 2024 - Data Protection Authority: In public contests the Public Administrations may only publish online the final rankings of the winners, under penalty of unlawful disclosure of personal data.

---

12 June 2024 - Italian Data Protection Authority: FAQs released clarifying the legal prerequisites and modalities for the processing by Institutes for Hospitalization and Treatment of a Scientific Nature (IRCCS) of personal data collected for health care purposes for further research purposes.

---

6 June 2024 - European Court of Human Rights (ECHR): a judge who extracts personal data from a lawyer's mobile phone infringes Article 8 of the Human Rights Convention.

ARTIFICIAL INTELLIGENCE.

18 June 2024 - OECD: report on the use of Artificial Intelligence in the public sector and state government published.

---

13 June 2024 – EU AI Act signed by the President of the European Parliament and the President of the Council of the European Union.

---

10 June 2024 - European Union: more than 1.7 million high-value public data for Artificial Intelligence training accessible on Open Data portal using quality datasets.

DIGITAL MARKETS.

5 June 2024 – Italian Antitrust Authority fines Meta €3.5M for violations of the Italian Consumer Code.

INFORMATION TECHNOLOGY

11 June 2024 - The Italian Government approves the legislative decree transposing Directive 2022/2555 (NIS 2) on measures for a high common level of cybersecurity in the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 1).

INDUSTRIAL PROPERTY - TRADEMARKS

5 June 2024 – EU General Court: McDonald's loses the EU trademark "*Big Mac*" in respect of poultry products.

DATA PROTECTION

17 June 2024 - Italian Data Protection Authority: published the final guideline on the processing and storage of e-mail metadata of public and private workers.

Following the public consultation launched by the Italian Data Protection Authority on the guideline document *'Computer programmes and services for the management of e-mail in the work context and the processing of metadata'*, on 6 June the same Authority issued the final document with the amended indications for public and private employers, recalling however that *'given the guideline document's indicative nature, no new obligations or responsibilities derive from it*'.
The Italian Data Protection Authority further clarifies what is meant by 'metadata' for the purposes of the Guideline Document: technically, this corresponds to the information recorded in the logs generated by the server systems for managing and sorting electronic mail (MTA = Mail Transport Agent) and by the workstations in the interaction that takes place between the various interacting servers and, where applicable, between these and the clients (the terminal workstations that send the messages and allow consultation of incoming correspondence by accessing the electronic mailboxes, defined in the technical standards as MUA - Mail User Agent). This information relating to the operations of sending and receiving and sorting messages may include the email addresses of the sender and the recipient, the IP addresses of the servers or clients involved in routing the message, the times of sending, retransmission or receipt, the size of the message, the presence and size of any attachments and, in certain cases, depending on the management system of the email service used, even the subject of the message sent or received. The metadata referred to in the document (both those of purely technical origin and those, such as the 'Subject' field, determined by users) then have the characteristic of being automatically recorded by the e-mail systems, regardless of the perception and will of the user. Finally, the provision clarifies that metadata are not to be confused with the information contained in the body of the e-mail message, even when they are technical information embedded in it or represent the set of structured technical headers documenting the routing of the message, its origin and other technical parameters. The information contained in the envelope, even if it corresponds to metadata automatically recorded in the logs of mail services, is inseparable from the message of which it is an integral part, which remains under the exclusive control of the user (whether the sender or the recipient of the messages).
Turning to the useful indications for data controllers for proper accountability, the Italian Data Protection Authority clarifies that the activity of collecting and storing only the metadata/logs necessary to ensure the operation of the e-mail system infrastructure falls under Article 4(2) of the Workers' Statute (thus not requiring trade union agreement or authorisation) if the storage period does not exceed 21 days. Any retention for an even longer period may be made, only in the presence of particular conditions that make it necessary to extend it, adequately demonstrating, in application of the accountability principle laid down in Article 5(2) of the GDPR, the specificities of the technical and organisational reality of the holder. On the contrary, the generalised collection and storage of e-mail logs, for a longer period of time, as it may entail an indirect remote control of workers' activities, requires the exercise of the guarantees provided for in Article 4(1) of Law No. 300/1970.

---

13 June 2024 – EU: Multistakeholder Expert Group to Commission publishes evaluation of the GDPR.

The Multistakeholder Expert Group on the General Data Protection Regulation (GDPR) to the European Commission published its report on the application of the GDPR.

In particular, the report highlights positive developments including an increase in data protection compliance and awareness of data protection rules, alongside greater controls for individuals over their data. The report outlined increased use of the right to access and right to erasure but conceded that there is still a lack of awareness among data subjects about their rights and how to exercise them in practice. Notably, with regard to the right not to be subject to automated decision-making under Article 22 of the GDPR, the report asked for greater clarity on the interplay between the GDPR and the EU Artificial Intelligence Act (AI Act).

The report also considered concerns that the exercise of the right not to be subject to automated decision-making raised competition issues and worries amongst businesses that explaining automation could reveal sensitive information and jeopardize business secrets. On data portability, the report suggested that the lack of awareness of data portability owes to the potential absence of standardization of data formats and the potential risk that in porting data to another organization, organizations may affect the rights and freedoms of others.

The report also notes concerns about the application of data protection principles under the GDPR, including data minimization and storage limitation. Likewise, the report detailed that many organizations are concerned about compliance with transparency obligations under the GDPR, particularly in the use of vague or overcomplicated terms considered not to be in line with the GDPR.

In addition, the report noted concerns surrounding the application of the GDPR in line with other regulations, such as the EU's anti-money laundering (AML) obligations and the Payment Services Directive (PSD2). Likewise, concerns were made apparent surrounding the adoption of Standard Contractual Clauses (SCCs) for data transfers to controllers and processors outside the EU whose processing is subject to the GDPR because of legal ambiguity surrounding applicable requirements which have not yet been addressed by the European Data Protection Board (EDPB). The issue is further complicated by potentially conflicting advice issued by national data protection authorities on cross-border data transfers. The report noted similar concerns on the enforcement of the GDPR in cross-border cases, and that lack of coordination between data protection authorities and differences in national procedures resulted in slow and inconsistent decisions.

---

12 June 2024 - Italian Data Protection Authority: favourable opinion on the draft Regulation for PA digital infrastructures and cloud services prepared by the Agency for National Cybersecurity (ACN).

The draft Regulation, which replaces the act previously adopted by the Agency for Digital Italy (AGID), takes into account the indications provided by the Guarantor in the course of the interlocutions. The document introduces a new article dedicated to the correct application of privacy regulations, which aims to ensure control, on the part of public administrations, over all those involved in data processing. In particular, it assigns PAs the role of data controllers, while digital infrastructure operators and cloud service providers are indicated as data processors.

The text also establishes the obligation for data controllers to adopt measures to ensure that administrations are promptly and adequately informed in the event of a data breach, given the volume and sensitivity of the data processed (health data, tax data). Data controllers will then have to provide PAs with appropriate tools to monitor the processing activities carried out by any sub-processors.

With regard to data transfers outside the European Economic Area, data controllers will be required to comply with the instructions of the administrations and to make available to them any information necessary to assess the effectiveness of the measures adopted.

The Regulation is part of the Italian Cloud Strategy, put in place by the Department for Digital Transformation and ACN, which contains the guidelines for the migration path towards the cloud of data and digital services of the Public Administration, also thanks to the National Strategic Pole (PSN), as a cloud infrastructure built on the impetus of the government.

---

12 June 2024 - Data Protection Authority: In public contests the Public Administrations may only publish online the final rankings of the winners, under penalty of unlawful disclosure of personal data.

Publishing on the web the results of intermediate tests or the personal data of competitors who have not won or have not been admitted to a contest is a breach of the data protection rights.

This is how the Italian Data Protection Authority ruled following a complaint lodged by a participant in a public contest organized by the Italian Institute per Social Security (INPS).

The complainant had complained about the publication on the Institute's website of numerous acts and documents, including the lists of those admitted and not admitted to the written test and oral test, and the list of participants, containing the assessment of qualifications by the Contest Committee, with an indication of the marks awarded to each candidate. These documents would then also end up on social networks by third parties.

The Italian Data Protection Authority recalled that Public Administrations, when they operate in the performance of contests procedures, must process the personal data of the persons concerned in compliance with the applicable sector regulations, and therefore it is not possible to publish online data of participants in competitions that are not required by law. In fact, differentiated levels of protection of personal data are not allowed, neither on a territorial basis nor at the level of individual administrations, especially when the matter has already been balanced and regulated by the legislator with uniform provisions at national level.

In quantifying the amount of the fine to INPS at EUR 20,000, the Authority took into account the nature, duration and seriousness of the breach, as well as the large number of persons concerned and the cooperative attitude of the Institute, which removed the lists in question, albeit following the Italian Data Protection Authority's request for information.

---

12 June 2024 - Italian Data Protection Authority: FAQs released clarifying the legal prerequisites and modalities for the processing by Institutes for Hospitalization and Treatment of a Scientific Nature (IRCCS) of personal data collected for health care purposes for further research purposes.

What are IRCCSs? How can they use personal data collected for the treatment of patients for research purposes? What obligations do they have under the Italian Data Protection Code? These questions have been answered by the Italian Data Protection Authority Privacy with FAQs.

The Authority's clarifications are addressed to IRCCSs, i.e. those bodies of the National Health Service that, according to standards of excellence, pursue research purposes in the biomedical field and in that of the organisation and management of health services, and perform highly specialised hospitalisation and care services.

In the FAQs it is explained that IRCCSs, in order to be able to use their patients' data also for the scientific research activity authorised by the Ministry, must identify an appropriate legal basis to legitimise such processing and an appropriate exception to the general ban on processing health and genetic data.

The Italian Data Protection Authority has therefore clarified that public and private IRCCSs, in addition to the consent of the research participants, may base the processing of personal data collected for the purpose of treatment for further research purposes on Article 110-bis, paragraph 4 of the Italian Data Protection Code, according to which the processing of data collected for clinical activity does not constitute further processing for research purposes.

However, if IRCCSs make use of this provision, they are obliged to carry out the Impact Assessment (DPIA) and publish it on their websites. However, if the full publication of the DPIA may infringe intellectual property rights, trade secrets or otherwise, the Institute may publish it in excerpts.

A specific section of the FAQs is devoted to the different ways of informing research participants depending on whether the data are collected from them or from the institute's internal databases or other participating centres.

Finally, the Authority has clarified the objective scope of application of Article 110-bis, paragraph 4 of the Code, which concerns all types of medical, biomedical, epidemiological, prospective and retrospective research, promoted by IRCCSs, including multicentre studies, whether carried out within the research

networks of IRCCSs or in those promoted by such institutes with the participation of entities that do not enjoy such recognition.

---

6 June 2024 - European Court of Human Rights (ECHR): a judge who extracts personal data from a lawyer's mobile phone infringes Article 8 of the Human Rights Convention.

The case concerns the conduct of a judicial investigation by a French magistrate seconded to the Monegasque courts. The applicant is a lawyer whose client was accused by her of secretly recording a conversation during a private meal. After reporting the crime of violation of privacy, the applicant handed over her mobile phone to the police so that the recording of the crime could be examined, and her good faith proved.

The investigating judge, who had only been entrusted with the task of verifying the authenticity of the recording and examining the content of the conversation in the light of Monegasque criminal law, decided instead to initiate a wide-ranging telephone investigation, without any real limitation in terms of time or scope of the search, thus allowing an 'exploratory' investigation to be carried out.

The European Court of Human Rights held that the investigations undertaken by the investigating judge into a lawyer's mobile phone and the massive and indiscriminate retrieval of personal data, including previously deleted data, went beyond the scope of the warrant, which concerned only acts of invasion of privacy, and that these exorbitant investigations were not accompanied by safeguards respecting the applicant's status as a lawyer and professional secrecy.

ARTIFICIAL INTELLIGENCE.

18 June 2024 - OECD: report on the use of Artificial Intelligence in the public sector and state government published.

With the publication of the Report *Governing with Artificial Intelligence: are governments ready?* the OECD reinforces its strategy - part of a broader effort - to ground the responsible use of AI in the public sector, especially in a number of key government functions. The report is very interesting and aims at knowledge sharing, exchange of best practices and structured policy dialogue between member states to understand the implications and guide responsible use of AI in the public sector. It is a document that underlines the growing realisation that, if used strategically and responsibly, artificial intelligence, including generative AI, has the potential to transform the way governments function, design policies and deliver services. The perspective is also particularly original: while the global debate on AI tends to focus on the role of governments as promoters, funders and - above all - regulators in shaping and responding to the application of AI, the report also focuses on states as users and, in some cases, developers of AI.

---

13 June 2024 – EU AI Act signed by the President of the European Parliament and the President of the Council of the European Union.

The President of the European Parliament and the President of the Council of the European Union signed the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (the AI Act).

The AI Act would apply to:

- providers placing on the market or putting into service artificial intelligence (AI) systems or placing on the market general-purpose AI (GPAI) models in the EU, irrespective of whether those providers are established or located within the EU or in a third country;
- deployers of AI systems that have their place of establishment or are located within the EU;
- providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the EU;

- importers and distributors of AI systems;
- product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark;
- authorized representatives of providers, which are not established in the EU; and
- affected persons in the EU.

The AI Act provides certain exemptions, including for systems used exclusively for military and defense as well as for research purposes.

Classification of AI systems

The AI Act takes a risk-based approach and prohibits certain AI practices, including cognitive behavioural manipulation, social scoring, AI for predictive policing based on profiling, and systems that use biometric data to categorize people according to specific categories such as race, religion, or sexual orientation.

Further, the AI Act classifies certain AI systems as high-risk and specifies requirements for high-risk AI systems, including the obligations of different entities. Notably, high-risk AI systems deployed by some entities providing public services would require a fundamental rights impact assessment.

The AI Act also regulates GPAI systems, and systems not posing systemic risks will be subject to limited requirements, for example with regard to transparency. However, those with systemic risks will have to comply with additional rules.

Enforcement and penalties

The AI Act would set up the following governing bodies:

- an AI Office within the Commission to enforce the common rules across the EU;
- a scientific panel of independent experts to support the enforcement activities;
- an AI Board with Member States' representatives to advise and assist the Commission and Member States on consistent and effective application of the AI Act; and
- an advisory forum for stakeholders to provide technical expertise to the AI Board and the Commission.

The AI Act provides different thresholds for fines and is set as a percentage of the company's global annual turnover in the previous financial year or a predetermined amount, whichever is higher. Small and medium-sized enterprises (SMEs) and start-ups are subject to proportional administrative fines. Specifically, non-compliance with the prohibition of the AI practices referred to in Article 5 of the AI Act would be subject to administrative fines of up to €35 million or, if the offender is an undertaking, up to 7% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

Next steps

The AI Act must now be published in the EU's Official Journal, after which it will enter into force 20 days after its publication and will apply two years after its entry into force, with some exceptions for specific provisions.

---

10 June 2024 - European Union: more than 1.7 million high-value public data for Artificial Intelligence training accessible on Open Data portal using quality datasets.

The EU's new rules to make nearly 1.7 million public data sets considered *'high-value datasets'* on six thematic areas established by the Open Data Directive - geospatial, earth observation and environment, meteorological, statistics, business and mobility - available for re-use via the official portal accessible here have officially entered into force.

These data can be freely used for machine learning in AI systems, promoting the development of new innovative products and services in those areas.

DIGITAL MARKETS.

5 June 2024 – Italian Antitrust Authority fines Meta €3.5M for violations of the Italian Consumer Code.

The Italian Competition Authority (AGCM) issued its decision in which it imposed a fine of €3.5 million on Meta Platforms Inc. and Meta Platforms Ireland Ltd. for unfair commercial practices constituting a violation of the Italian Consumer Code.

The AGCM noted that after receiving some reports, it had started a preliminary investigation on April 28, 2023. The AGCM stated that the following claims were being investigated: (1) in relation to new Instagram users, the information provided to new users related to the collection and use of their data for commercial purposes, including information generated by the user's use of other Meta apps and third-party websites/apps was incomplete; (2) in relation to existing Instagram and Facebook users: Meta did not provide adequate notice and justification for the suspension of accounts; and Meta did not provide adequate and effective assistance to recover accounts in cases where users are no longer able to access such accounts.

The AGCM found that Meta had not provided users with clear information during the registration phase regarding the collection and use of their personal data for commercial purposes. Additionally, it found that with existing users, in the event of Facebook and Instagram accounts getting suspended, no useful communication was provided to users relating to how Meta decides to suspend accounts or the possibility of contesting the suspension.

In light of the above, the AGCM concluded that Meta violated Articles 20, 21, and 22 of the Italian Consumer Code and imposed a fine of €3.5 million.

INFORMATION TECHNOLOGY

11 June 2024 - The Italian Government approves the legislative decree transposing Directive 2022/2555 (NIS 2) on measures for a high common level of cybersecurity in the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 1).

The NIS2 directive is the EU's cyber security legislation. It provides legal measures to strengthen the overall level of cyber security in the EU. Compared to the previous 2016 Directive (NIS 1), it modernised the existing legal framework to keep pace with increased digitisation and an evolving cybersecurity threat landscape, extending the scope of cybersecurity rules to new sectors and entities and further enhancing the resilience and incident response capabilities of public and private entities, competent authorities and the EU as a whole.

The NIS 2 Directive introduces a renewed security culture in all sectors that are vital to the European economy and society and heavily dependent on Information and Communication Technologies (ICT), such as energy, transport, water, banking and financial market infrastructures (it has to be reminded that that the NIS 2 Directive shall not apply to banking financial and insurance entities required to comply with DORA Regulation 2022/2554 on digital operational resilience, a *lex specialis* of the sector), healthcare and digital infrastructures (ICT providers are also subject to the aforementioned DORA Regulation).

The Italian legislative decree intervenes by introducing the following main innovations (the deadline for Member States to transpose the NIS 2 Directive is 17 October 2024):

- the widening of the subjective scope of application
- the distinction between "essential subjects" and "important subjects" and the adoption of a dimensional criterion for their identification (to overcome the serious subjective limits in the identification of the subjects required, given that NIS 1 left the Member States free to identify national criteria, resulting in a fragmentation of the rules)
- the streamlining of minimum security requirements and mandatory notification procedures;
- the adoption of a 'multi-risk' approach;
- the regulation of coordinated vulnerability disclosure (CVD) and the specific coordination functions assigned to national CSIRTs;
- the implementation of cooperation measures to support the coordinated management of large-scale cybersecurity incidents and crises at the operational level.

INDUSTRIAL PROPERTY - TRADEMARKS

5 June 2024 – EU General Court: McDonald's loses the EU trademark "*Big Mac*" in respect of poultry products.

The General Court holds that McDonald's has not proved genuine use within a continuous period of five years in the European Union in connection with certain goods and services.

Supermac's and McDonald's, an Irish and American fast-food chain respectively, are involved in a dispute regarding the EU trademark Big Mac. That trademark had been registered for McDonald's in 1996. In 2017, Supermac's filed an application for revocation of that mark in relation to certain goods and services.

It submitted that the mark had not been put to genuine use in the European Union in connection with those goods and services within a continuous period of five years. The European Union Intellectual Property Office (EUIPO) partially upheld that application. However, it confirmed the protection which the contested mark conferred on McDonald's in respect of, inter alia, foods prepared from meat and poultry products and meat and chicken sandwiches as well as in respect of services rendered or associated with operating restaurants and other establishments or facilities engaged in providing food and drink prepared for consumption and for drive-through facilities and also the services of the preparation of carry-out foods.

By its judgment, the General Court partially annuls and alters EUIPO's decision, thus further limiting the protection conferred on McDonald's by the contested mark. The General Court holds that McDonald's has not proved that the contested mark has been put to genuine use as regards the goods 'chicken sandwiches', the goods 'foods prepared from poultry products' and the 'services rendered or associated with operating restaurants and other establishments or facilities engaged in providing food and drink prepared for consumption and for drive-through facilities; preparation of carry-out foods'. The evidence which was submitted by McDonald's does not provide any indication of the extent of use of the mark in connection with those goods, as regards the volume of sales, the length of the period during which the mark was used and the frequency of use. Consequently, the evidence taken into account by EUIPO does not serve to prove that there has been genuine use of the contested mark in connection with those goods. Furthermore, the evidence submitted by McDonald's does not serve to prove that the contested mark has been used in connection with 'services rendered or associated with operating restaurants and other establishments or facilities engaged in providing food and drink prepared for consumption and for drive-through facilities; preparation of carryout foods