FIVERS

Regulatory update

Data protection, IP, IT e AI

n. 3 / 2024

DATA PROTECTION

3 June 2024 - Supreme Court of Cassation: requirements for the lawful processing of personal data relating to an employee's travels taken from the Telepass system.

---

1 June 2024 - Italian Data Protection Authority: if the employee is undeclared, personal data disclosed to the undeclared employee are automatically processed unlawfully.

---

31 May 2024 - Artificial Intelligence: the Italian Data Protection Authority Issues Guidance to Protect Personal Data from Web Scraping.

---

27 May 2024 - European Data Protection Board – EDPB announces adoption of the report on the work of the ChatGPT taskforce.

---

27 May 2024 - *Statement* by the European Data Protection Board on the Financial Data Access and Payments Package.

ARTIFICIAL INTELLIGENCE.

3 June 2024 – The European Data Protection Supervisor – EDPS enacts Guidelines for the use of Generative AI in compliance with the data protection rules for public bodies.

---

31 May 2024 - The EU Commission inaugurates the Office for Artificial Intelligence.

---

23 May 2024 – Council reaches political agreement on the use of super-computing for AI development.

DIGITAL MARKETS.

31 May 2024 - EU Court of Justice - E-commerce: a Member State may not impose additional obligations on an online service provider established in another Member State.

---

24 May 2024 – EU Commission calls on 18 Member States to comply with the EU Data Governance Act.

INFORMATION TECHNOLOGY

31 May 2024 - EU Court of Justice: Online orders, the order button, or a similar function, must clearly indicate that, by clicking on it, the consumer assumes an obligation to pay.

---

24 May 2024 – New options within he electronic platform for conducting mediation proceedings on line.

---

22 May 2024 - Supreme Court of Cassation: an ordinary e-mail message cannot be excluded from evidentiary relevance merely because it is not digitally signed.

DATA PROTECTION

3 June 2024 - Supreme Court of Cassation: requirements for the lawful processing of personal data relating to an employee's travels taken from the Telepass system.

With Order No. 15391 of 3 June 2024, the Court of Cassation specified the requirements under which the employer may legitimately process data from the Telepass system installed on the company car. A company technician had been dismissed for objective justification, having disclosed geolocation data (taken from a PDA in use by the employee and from the movements recorded at the toll booths by the Telepass system) omissions and failure to perform work activities. While the Court of First Instance had rejected the application for the annulment of the dismissal, the Court of Appeal had held that the data taken from the Telepass system could not be used for an illegitimate - albeit ex post - remote control of the worker because it was not based on 'adequate information' within the meaning of Article 4(3) of the Workers' Statute, which permits the use 'for any purpose of the employment relationship' of personal data collected by means of control instruments provided that the worker is given adequate information about 'the manner of use of the instruments and the performance of the controls' and that the conditions set out in the Privacy Code (*rectius*: by the applicable data protection legislation). Since the employer had failed to provide the due information of transparency on the installation of the Telepass on the company car (even though it was a work tool assigned to the transfer technician for the performance of his duties), the Court held that the data on which the dismissal was based were unusable (whereas the employer had correctly processed the data taken from the PDA, for which there was both the specific privacy notice and the correct setting pursuant to Article 4 of the Workers' Statute). Therefore, the Court of Cassation once again emphasised the fundamental importance of transparency vis-à-vis employees as a discriminating factor between lawful and unlawful collection of data and between remote control that complies or does not comply with Article 4 of the Workers' Statute.

---

1 June 2024 - Italian Data Protection Authority: if the employee is undeclared, personal data disclosed to the undeclared employee are automatically processed unlawfully.

An important measure by the Italian Data Protection Authority, which in its order-injunction 243/2024 affirmed a principle with a significant practical impact: the irregularity of the employment relationship corresponds to the violation of privacy. In fact, if a worker is irregular, he is not part of the organisational structure of the data controller and is not entitled to process personal data as an authorised processor. The irregular worker is even a third party to whom the data are unduly communicated.

Thus, in addition to labour sanctions, undeclared work is also likely to result in sanctions for violation of data protection law.

---

31 May 2024 - Artificial Intelligence: the Italian Data Protection Authority Issues Guidance to Protect Personal Data from Web Scraping.

The Italian Data Protection Authority (Garante) has issued guidance on how to protect personal data published online by public and private entities in their capacity as data controllers from web scraping, i.e. the indiscriminate collection of personal data on the internet, carried out by third parties for the purpose of training generative artificial intelligence (GAI) models. The guidance reflects the contributions obtained by the Garante as part of its fact-finding investigation, approved last December.

While waiting to decide – following the outcome of a number of investigations already under way, including the one against OpenAI - on the lawfulness of web scraping of personal data performed on the basis of legitimate interest, the Garante deemed it necessary to provide data controllers who publish personal data online with initial guidance on the need to adopt appropriate security measures to prevent or, at least, hinder web scraping.

In the guidance document, the Garante suggests a number of concrete measures to be adopted: the creation of reserved areas, accessible only upon registration, so as to remove data from public availability; the inclusion of anti-scraping clauses in the terms of service of websites; the monitoring of traffic to web pages, so as to identify any abnormal flows of incoming and outgoing data; the implementation of specific measures against bots using, among others, the technological solutions made available by the same companies responsible for web scraping (e.g.: intervening on the robots.txt file).

These measures are not mandatory and data controllers shall assess, based on the principle of accountability, whether to implement them to prevent or mitigate, in a selective manner, the effects of web scraping, considering a number of elements such as the latest technology developments and the costs of implementation, in particular for SMEs.

---

27 May 2024 - European Data Protection Board – EDPB announces adoption of the report on the work of the ChatGPT taskforce.

The European Data Protection Board – EDPB adopted a report on the work of the ChatGPT taskforce. This taskforce was created by the EDPB to promote cooperation between Data Protection Authorities (DPA) investigating the chatbot developed by OpenAI. The report provides preliminary views on certain aspects discussed between DPAs and does not prejudge the analysis that will be made by each DPA in their respective, ongoing investigation.

The report analyses several aspects concerning common interpretation of the applicable GDPR provisions relevant for the various ongoing investigations, such as:

- lawfulness of collecting training data ("web scraping"), as well as processing of data for input, output and training of ChatGPT.
- fairness: ensuring compliance with the GDPR is a responsibility of OpenAI and not of the data subjects, even when individuals input personal data.
- transparency and data accuracy: the controller should provide proper information on the probabilistic nature of ChatGPT's output and refer explicitly to the fact that the generated text may be biased or made up.

The report points out that it is imperative that data subjects can exercise their rights effectively.

Taskforce members also developed a common questionnaire as a possible basis for their exchanges with Open AI, which is published as an annex to the report.

Furthermore, the EDPB decided to develop guidelines on Generative AI, focusing as a first step on data scraping in the context of AI training.

---

27 May 2024 - *Statement* by the European Data Protection Board on the Financial Data Access and Payments Package.

On 28 June 2023, the EU Commission published a legislative package ('Financial Data Access and Payments Package - FIDAP') of three proposals concerning payments and access to financial data:

(1) a proposal for a Financial Data Access Regulation (FIDA) Framework Regulation;

(2) a proposal for a Payment Services Regulation (PSR); and

(3) a proposal for a Payment Services Directive (PSD3).

FIDAP's common goal is to improve consumer protection and competition in the area of electronic payments, and to enable consumers to share their financial data to access a wider range of more convenient financial products and services. Following its 2023 Opinions on the various legislative proposals, the EDPB issued on 27 May a Statement highlighting the issues on which further alignment is needed between the legislative proposals (which will preferably be taken up with the new EU legislature), the guidelines adopted by the European Data Protection Supervisor, and - indeed - the various Opinions already issued by the EDPB. This is to ensure a higher level of personal data protection than that already provided by the additions made by the EU Parliament. The Statement is of particular interest because it provides further indications (in addition to those contained in the EDPB Opinions of 2023) on the processing of personal data implied by the three regulatory proposals that outline a market that will be fundamental in the coming years: that of the use of data derived from the use of financial services to build innovative apps and services.

ARTIFICIAL INTELLIGENCE.

3 June 2024 – The European Data Protection Supervisor – EDPS enacts Guidelines for the use of Generative AI in compliance with the data protection rules for public bodies.

The EDPS has published its Guidelines on generative Artificial Intelligence and personal data for EU institutions, bodies, offices and agencies (EUIs). The guidelines aim to help EUIs comply with the data protection obligations set out in Regulation (EU) 2018/1725, when using or developing generative AI tools.

The guidelines on generative AI are a first step towards more extensive recommendations in response to the evolving landscape of generative AI tools, with the aim of covering as many possible scenarios involving the use of generative AI, to provide enduring advice to EUIs so that they can protect individuals' personal information and privacy.
To ensure their practical application by EUIs, the guidelines emphasise on data protection's core principles, combined with concrete examples, as an aid to anticipate risks, challenges and opportunities of generative AI systems and tools.

As such, the guidelines focus on a series of important topics, including advice on how EUIs can distinguish whether the use of such tools involves the processing of individuals' data; when to conduct a data protection impact assessment; and other essential recommendations.

The EDPS issues these guidelines within its role as independent data protection authority of the EUIs, so that they comply with the EU's data protection law applicable to them, in particular Regulation (EU) 2018/1725. The EDPS has not issued these guidelines within its role as AI Supervisor of the EUIs under the EU's Artificial Intelligence Act for which a separate strategy is being prepared.

---

31 May 2024 - The EU Commission inaugurates the Office for Artificial Intelligence.

The European AI Office will support the development and use of trustworthy AI, while protecting against AI risks. The AI Office was established within the European Commission as the centre of AI expertise and forms the foundation for a single European AI governance system.

The EU aims to ensure that AI is safe and trustworthy. For this purpose, the AI Act is the first-ever comprehensive legal framework on AI worldwide, guaranteeing the health, safety and fundamental rights of people, and providing legal certainty to businesses across the 27 Member States.

The AI Office is uniquely equipped to support the EU's approach to AI. It will play a key role in implementing the AI Act by supporting the governance bodies in Member States in their tasks. It will enforce the rules for general-purpose AI models. This is underpinned by the powers given to the Commission by the AI Act, including the ability to conduct evaluations of general-purpose AI models, request information and measures from model providers, and apply sanctions. The AI Office also promotes an innovative ecosystem of trustworthy AI, to reap the societal and economic benefits. It will ensure a strategic, coherent and effective European approach on AI at the international level, becoming a global reference point.

For a well-informed decision-making**,** the AI Office collabo**rates** with Member States and the wider expert community through dedicated fora and expert groups**.** These combine knowledge from the scientific community, industry, think tanks, civil society, and the open-source ecosystem, ensuring that their views and expertise are taken into account. Grounded in comprehensive insights of the AI ecosystem, including advances in capabilities, deployment and other trends, the AI Office fosters a thorough understanding of potential benefits and risks.

---

23 May 2024 – Council reaches political agreement on the use of super-computing for AI development.

The Council has reached a political agreement on a regulation to expand the objectives of the European High Performing Computer Joint Undertaking (EuroHPC), aimed at boosting Europe's leadership in artificial intelligence (AI). The regulation adds an additional objective for the Joint Undertaking: to develop and operate AI Factories in support of an artificial intelligence ecosystem in the Union. AI Factories will be entities that provide AI super-computing service infrastructure. The regulation will also make the Union's supercomputing capacity further available to innovative AI European startups to train their models.

In particular, the Council agreement ensures that the activities covered by the AI Factories provide fair access opportunities to the AI-optimised supercomputers, opening them up to a larger number of public and private users.

The regulation explicitly mentions start-ups and small and medium-sized enterprises as possible beneficiaries of the AI-super-computers. They will be able to use the one-stop-shop that each hosting entity creates to facilitate access to its support services. The Council position calls on the EuroHPC Governing Board to define special access conditions for the AI-super-computers, including dedicated access to start-ups and SMEs.

Following the political agreement, hosting entities can receive a Union financial contribution that covers up to 50% of the acquisition costs of AI-super-computers and up to 50% of their operating costs (including AI-oriented super-computing service costs). The ownership of the AI-optimised supercomputers can be transferred to the hosting entities five years after the machine has passed an acceptance test.

Finally, the regulation states that the AI-super-computers should primarily be used to develop, test, evaluate and validate large-scale, general-purpose AI training models and emerging AI applications, and to further develop AI solutions in the Union.

The new Regulation will be published in the Official Journal after legal review. This regulation will enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

DIGITAL MARKETS.

31 May 2024 - EU Court of Justice - E-commerce: a Member State may not impose additional obligations on an online service provider established in another Member State.

In Italy, providers of online intermediation services and search engines, such as Airbnb, Expedia, Google, Amazon and Vacation Rentals, are subject to certain obligations under national provisions. They were adopted in 2020 and 2021, with the stated aim of ensuring the adequate and effective enforcement of the regulation on promoting fairness and transparency for business users of online intermediation services 1 . Providers of those services must, inter alia, be entered in a register held by an administrative authority (AGCOM), periodically forward to it a document on their economic situation, provide it with a series of detailed information and pay it a financial contribution. Penalties are provided for in the event of failure to comply with those obligations. The above-mentioned companies are challenging those obligations before an Italian court, on the grounds that the resulting increase in administrative charges is contrary to EU law 2 . All those companies – except for Expedia, which is established in the United States – invoke the principle of freedom to provide services and argue that they are mainly subject to the legal system of the

Member State in which they are established (in this case, Ireland or Luxembourg). Therefore, they consider that Italian law cannot impose on them other requirements relating to access to the activity of information society services. In that context, the Italian court decided to refer the matter to the Court of Justice. The Court of Justice holds that EU law precludes measures such as those adopted by Italy. Under the Directive on electronic commerce, it is the home Member State of the company providing information society services that regulates the provision of those services. Member States of destination, bound by the principle of mutual recognition, are required, save in exceptional circumstances, not to restrict the freedom to provide those services. Thus, Italy cannot impose on providers of those services established in other Member States additional obligations which, although required for the provision of those services in that country, are not imposed in their Member State of establishment. According to the Court of Justice, those obligations do not fall within the exceptions permitted by the Directive on electronic commerce. First, they are, subject to verification by the Italian court, of general and abstract application. Secondly, they are not necessary in order to protect one of the objectives of general interest referred to in that directive. Moreover, the establishment of those obligations is not justified by the intention, invoked by the Italian authorities, to ensure the adequate and effective enforcement of the above-mentioned regulation.

---

24 May 2024 – EU Commission calls on 18 Member States to comply with the EU Data Governance Act.

The European Commission decided to open infringement procedures by sending a letter of formal notice to 18 Member States that did not designate the responsible authorities to implement the Data Governance Act, or that have failed to prove that the latter are empowered to perform the tasks required by the Act.

Those member states are: Belgium, Czechia, Germany, Estonia, Greece, France, Italy, Cyprus, Latvia, Luxembourg, Malta, Austria, Poland, Portugal, Romania, Slovenia, Slovakia and Sweden.

The Data Governance Act facilitates data sharing across sectors and EU countries for the benefit of citizens and businesses. It will increase trust in data sharing by establishing rules for neutrality of data intermediaries that connect individuals and companies with data users. Data intermediation activities have to be strictly independent of any other services that they provide, be registered and can be identified by a common EU logo. The Act will also facilitate the reuse of certain data held by the public sector and stimulate voluntary sharing of data. Data altruism allows citizens to give their consent to make available data that they generate for the common good, for example for medical research projects. Data altruism organisations can decide to be included in a public register and use the common EU logo. They must have a not-for-profit character and meet transparency requirements as well as offer specific safeguards to protect the rights and interests of citizens and companies that decide to share their data. Applicable since 24 September 2023, the responsible authorities are in charge of the registration of data altruism organisations and of monitoring the compliance of data intermediation services providers. The Commission is therefore sending a letter of formal notice to the 18 Member States concerned which now have 2 months to respond and address the shortcomings raised by the Commission. In the absence of a satisfactory response, the Commission may decide to issue a reasoned opinion.

INFORMATION TECHNOLOGY

31 May 2024 - EU Court of Justice: Online orders, the order button, or a similar function, must clearly indicate that, by clicking on it, the consumer assumes an obligation to pay.

In Germany, the tenant of an apartment – the monthly rent of which was higher than the maximum ceiling permitted under national law – asked a debt recovery undertaking to request his landlords to repay rent overpayments. He placed that order through that service provider’s website. Before clicking on the order button, he ticked a box to accept the general terms and conditions. According to those terms and conditions, tenants must pay the service provider a third of the annual rent saved where that provider’s attempts to assert their rights were successful. In the ensuing dispute between the service provider and the landlords, the latter argue that the tenant did not give the service provider proper authorisation to act

on his behalf. Indeed, the order button was not labelled with the words “order with obligation to pay” (or a corresponding formulation), as required by the directive on consumer rights.
In that context, the question arose as to whether that requirement applies also where the tenant’s obligation to pay does not arise solely from the order, but in addition requires the successful enforcement of his or her rights. The German court seized of the dispute referred a question to the Court of Justice in that regard. The Court holds that the trader must inform, in accordance with the requirements of the Directive, the consumer before he or she places the order through the internet that he or she, by that order, assumes an obligation to pay. That obligation on the part of the trader applies irrespective of whether the consumer’s obligation to pay is unconditional or whether the consumer is required to pay the trader only after a subsequent condition has been satisfied. If the trader has not complied with his obligation to provide information, the consumer is not bound by the order. However, there is nothing to prevent the consumer from confirming his or her order.

---

24 May 2024 – New options within he electronic platform for conducting mediation proceedings on line.

In order to improve the functioning of the platform for conducting mediation proceedings in telematic mode, new functions are in place that enhance its usability. In particular, the system has been implemented with the following:

- the direct creation of meetings by the mediator: with this feature, the mediator can independently manage the meetings following the first one, duplicating the meeting that has just ended. The new meeting will inherit all the information contained in the original one except for the documents attached to it; the mediator will also be able to make changes regarding the associated parties;

- the extension of the types of documents for identification: participants may also be identified by their driving licence in addition to their identity card and passport;

- the visibility to the mediator: of those who have completed the digital signature process of the agreement;

- integration with other platforms: for ODM using Visura applications, integration with the Verbalsfera platform is active. Integration with DCS Software users using the Concilio platform will also be active shortly;

- the possibility for the mediator to disable the access of the parties with SPID or digital signature and thus allow access with a simple click on the link contained in the meeting convocation email.

---

22 May 2024 - Supreme Court of Cassation: an ordinary e-mail message cannot be excluded from evidentiary relevance merely because it is not digitally signed.

The Court of Cassation, section III Civil, in its judgment no. 14046 of 21 May 2024, dealt with the case of a haulier who had entered into an insurance contract through a broker against the risk of theft of the goods transported (a load of medicines). Theft then actually occurred with liability charged to the carrier. At the shipper's request to be indemnified for the damage, the carrier asked to be held harmless by the insurance company, which, however, denied the indemnity on the ground that the insurance contract excluded from coverage the damage resulting from the theft of medicines.

In the course of the proceedings, among the various objections, the haulier instead objected to the company's extension of the coverage to the risk of theft of medicines due to an exchange of e-mails between the broker (also sued) and an official of the company itself. At first instance, the Court of First Instance had upheld the claim against the company, arguing precisely on the basis of the exchange of e-mails. In the second instance, the Court of Appeal rejected the claim against the company on the grounds that the exchange of e-mails could not integrate the written form required by Article 1888 of the Civil Code since ‘it was an exchange of simple, ordinary e-mails and not an exchange by means of certified electronic mail’ and that the ordinary e-mail ‘has the value of a photocopy, rectius of a mechanical reproduction, and is full proof, pursuant to Article 2712 of the Civil Code, only if not contested’.

For the Supreme Court, on the other hand, the e-mail message is a computer document capable of satisfying the requirement of written form and freely assessable in court, taking into account its objective characteristics of quality, security, integrity and immodifiability. It follows that the judge cannot simply deny that an e-mail message with a ‘simple’ electronic signature satisfies the requirement of written form, but must first examine and assess its ‘*objective characteristics’ which, therefore, ‘must be deduced from the corpus mechanicum available to the judge: and therefore - in particular - from the format of the file in which the e-mail message was saved; from its properties; from the syntax adopted; from the graphics’*.

In summary, therefore, for the Supreme Court:

- the e-mail message signed with a ‘simple’ signature is a computer document within the meaning of Article 2712 of the Civil Code
- if its provenance or content are not disputed, it forms full evidence of the facts and things represented;
- if its provenance or content is disputed, the judge may not exclude that document from the list of usable evidence but must assess it in conjunction with all the other available elements and taking into account its intrinsic characteristics of security, integrity and immodifiability.