FIVERS

Regulatory update
Data protection, AI, IT and IP

No 20/2026

DATA PROTECTION

9 November 2026 - Italian Data Protection Authority: deleting data does not remedy the silence towards the data subject

---

5 November 2026 - EU Court of Justice: the file of a privacy complaint is not "inaccessible" to the complainant's data.

---

3 November 2026 - Italian Data Protection Authority: the deadline for adaptation for tracking pixels in e-mails has expired.

---

1 November 2026 – European Data Protection Board: public consultations on anonymisation and web scraping in generative AI closed.

ARTIFICIAL INTELLIGENCE

11 November 2026 – European Commission: Digital Fairness Act, new rules for AI agents, chat-bots, digital contracts and manipulative business practices.

---

9 November 2026 – AgID: the final Guidelines on artificial intelligence in the PA have been published. Governance, risk management, data protection and controls obligations on the systems adopted.

---

3 November 2026 - Advocate General of the Court of Justice of the EU: when a chatbot uses press articles to respond to users, it can affect publishers' rights.

CYBERSECURITY

6 November 2026 – Department for Digital Transformation: technical specifications adopted to test the IT-Wallet.

---

25 October 2026 – National Agency for Cybersecurity - ACN: simplified NIS 2027 registration for already registered subjects, but only if the data have not changed.

INFORMATION TECHNOLOGY

10 November 2026 - Campania Regional Administrative Court, Salerno: in online tenders, the upload of documents is not enough to submit the bid.

DIGITAL MARKETS

5 November 2026 - EU Court of Justice: the smart meter is not optional for the sole fact that the customer prefers a traditional meter.

INTELLECTUAL AND INDUSTRIAL PROPERTY

4 November 2026 – EU General Court: in short marks, a common word is not enough to demonstrate the likelihood of confusion.

DATA PROTECTION

9 November 2026 - Italian Data Protection Authority: deleting data does not remedy the silence towards the data subject

A university removed the data of a former student contained in an electoral roll from its website, but had not responded to his request for deletion. It had also left two subsequent invitations from the Authority unanswered, communicating the removal only after the start of the sanctioning procedure. The Authority ascertained the violation of art. 5, 12 and 17 GDPR and imposed a fine of 4,000 euros on the University.

The decision highlights two distinct obligations. The controller must assess and, when the conditions are met, execute the request for erasure; it must also notify the data subject of what it has done, without undue delay and in any case within one month of receiving the request. If it cannot accept it, it must explain the reason and indicate the possibility of contacting the Data Protection Authority or the judge. In the cases provided for by the GDPR, the deadline can be extended, but the data subject must be informed within the first month. The subsequent removal of the data does not eliminate the violation already accrued due to the lack of response.

For companies and PAs, the case suggests treating each privacy request as a traceable procedure: recording the date of receipt, assigning a person responsible for the response, verifying the outcome of the technical intervention and keeping evidence of both the action taken and the communication sent to the data subject. It is also necessary to monitor the Authority's requests separately: in the case examined, the lack of cooperation was considered by the Authority in determining the sanction.

---

5 November 2026 - EU Court of Justice: the file of a privacy complaint is not "inaccessible" to the complainant's data.

A person lodges a complaint with the data protection authority and then asks to know his or her personal data contained in the relevant file. Can the authority reject the request by invoking a rule that excludes access to his files en bloc? In *Bayerisches Landesamt für Datenschutzaufsicht* (C-205/25), the Court of Justice answered no. When processing the data collected and produced in the context of the complaint, the supervisory authority is itself the data controller: the complainant can therefore exercise the right of access under Article 15 GDPR against him, in principle.

However, the ruling makes a precise distinction between access to personal data and indistinct access to the entire administrative file. The former is protected by the GDPR; the latter does not automatically follow from Article 15. The authority must assess what information actually concerns the applicant and balance the request with the rights and freedoms of other persons. Where possible, the redaction or anonymisation of third-party data makes it possible to provide the necessary information without disclosing the information to be protected. Article 23 GDPR allows legislative limitations on the right of access only within its strict conditions: it does not justify a generalised exclusion of all personal data in the authority's files.

On an operational level, the ruling is primarily of interest to the supervisory authorities, which must be able to examine these requests individually and justify any limitations. It is also relevant for the companies involved in the investigation: documents, replies and attachments sent to the authority may contain data of the complainant together with third-party or confidential information. It is advisable to identify them accurately from the moment they are transmitted, so that the protection needs can be assessed concretely, without presuming that the placement in the file makes everything automatically ostensible or, on the contrary, everything secret.

Court of Justice of the EU, judgment of 5 November 2026, C205/25, ECLI:EU:C:2026:933.

---

3 November 2026 - Italian Data Protection Authority: the deadline for adaptation for tracking pixels in e-mails has expired.

On 29 October, the six-month deadline, starting from the publication in the Official Gazette of 29 April 2026, which the Authority had granted to comply with the guidelines on tracking pixels in email communications, expired. The guidelines had been adopted with provision no. 284 of 17 April 2026: they are not a new act issued in October, but the deadline makes the verification of campaigns already operational current.

Pixels can reveal the opening of a message and, depending on the configuration, collect additional information about the recipient. The Authority's indications also concern newsletters, automatic messages and service communications, not only advertising emails. The recipient must be informed in advance of the presence of tracking and its purposes. For the *individual* measurement of openings used, for example, to evaluate promotional campaigns, adapt the frequency of messages or build commercial profiles, the guidelines generally require prior consent. However, the Authority provides for exceptions to be evaluated concretely, including only aggregated and anonymous statistics, certain security requirements and specific institutional or service communications.

The verification for companies and PAs should start from the platform actually used: which pixels are active by default, what data they produce, whether they measure the individual recipient and who accesses them. It is then necessary to align information, collection and proof of consent, instructions to the supplier and revocation systems. The Authority allows, under certain conditions, a single informed consent for promotional messages and related tracking, but requires that the user can subsequently revoke even the tracking alone, continuing to receive pixel-free emails. For pre-existing processing, the guidelines provide for specific transitional procedures, not to be confused with a permanent exemption from obligations.

Italian Data Protection Authority, guidelines of 17 April 2026, published in the Official Gazette of 29 April 2026.

---

1 November 2026 – European Data Protection Board: public consultations on anonymisation and web scraping in generative AI closed.

The public consultation on the EDPB Guidelines 02/2026 on anonymisation, adopted in July in a version subject to consultation, has closed. The issue is relevant for those who share datasets, publish statistics, feed research environments or reuse data to develop AI systems: qualifying a set of information as "anonymous" means arguing that people are not identifiable according to the applicable legal criterion, not simply that names and tax codes have been removed.

In the draft, the EDPB proposes to examine the possibility of identification also from the perspective of individuals who could have the data and the means that could reasonably be used to combine it with other information. The Scoreboard considers three risks: isolating the record of a person, linking it to other data, and deriving information about them through inference. If one of these profiles remains open, further analysis is needed before declaring anonymisation successful.

On an operational level, companies and PAs should document which dataset has been assessed, in what context it will be made available and which entities could access it, reviewing the conclusion if data, recipients or available techniques change. The closure of the consultation, however, does not make the draft definitive and does not introduce a new regulatory threshold on 30 October: it is necessary to wait for the eventual final version of the EDPB.

The consultation on the EDPB Guidelines 03/2026 dedicated to automated data collection from the web for generative AI development has also ended. The draft, published in July, addresses a practical issue for developers, procurers and model providers: the availability of data on publicly accessible pages does not eliminate the application of the GDPR when the collection, storage or use concerns personal data.

The EDPB refers in particular to the need to define the purposes of the collection, identify a legal basis, respect transparency and minimization, and verify the accuracy of the data intended for training. The draft discusses the conditions for assessing legitimate interest, without considering it as an automatically available basis for any scraping. If the collection involves special categories of data, a condition of Article 9 GDPR must also be examined separately: there is no general exemption for sensitive data that appears incidentally on the web.

For organisations developing or purchasing AI solutions, the operational consequence is to ask for a verifiable reconstruction of the data sources, selection criteria, filters applied, quality controls and measures to manage surplus or sensitive data. The closure of the consultation is not equivalent to the final adoption of the guidelines; the draft remains a reference to anticipate the issues that the EDPB is examining, not a new framework that entered into force on 30 October.

EDPB consultation on Guidelines 02/2026 and EDPB communication of 8 July 2026. European Data Protection Board

EDPB consultation on Guidelines 03/2026 and EDPB communication of 8 July 2026.

ARTIFICIAL INTELLIGENCE

11 November 2026 – European Commission: Digital Fairness Act, new rules for AI agents, chatbots, digital contracts and manipulative business practices.

On 11 November 2026, the European Commission presented the proposal for a *Digital Fairness Act* Regulation (COM(2026) 1100 final), aimed at strengthening consumer protection in digital markets and combating commercial practices that unduly influence their decisions. The intervention proposes to replace Directive 2005/29/EC on unfair commercial practices with a Regulation directly applicable in the Member States, preserving its fundamental principles and introducing new provisions to address the risks arising from algorithmic personalization, digital interfaces and the use of artificial intelligence in consumer relations.

One of the main innovations concerns the prohibition of so-called *dark patterns*, i.e. interface design techniques that induce users to make commercial decisions that are not fully free and conscious. The proposal prohibits, among other things, misleading messages about the availability of products, artificial pressure to purchase and other forms of manipulation of choices. It also introduces a principle of *fairness by design*, which includes the possibility of disabling features designed to incentivize excessive or compulsive use of digital services. This provision also affects chatbots and AI assistants that simulate interpersonal relationships to prolong interactions with users.

Particularly innovative are the provisions dedicated to AI agents capable of selecting products, negotiating conditions and autonomously concluding contracts on behalf of consumers. The proposal provides that users can establish in advance whether to confirm all transactions, only certain categories of purchases or authorize the agent to operate without prior confirmation. It will be possible to define and modify parameters such as maximum amounts and time limits. Transparency obligations on remuneration and conflicts of interest are also envisaged, with the need for consumer confirmation in the cases indicated by the proposal. The regulation thus introduces specific guarantees for automated commerce, while providing for an exclusion for financial services.

New protections also concern automated assistance services and digital contracts. When post-contractual assistance is provided online, the consumer will be able to request to communicate with a human operator if the other tools are not effective, according to the conditions and exceptions provided for in the proposal. Measures are also introduced against subscriptions that are difficult to cancel, non-transparent automatic renewals and the transformation of free trials into paid services without express consent. Further provisions concern influencer marketing, personalized advertising aimed at minors, the exploitation of consumer vulnerabilities and price transparency, including when determined by algorithmic systems.

The new tools for monitoring and detecting infringements are also relevant. Article 34 of the proposal would allow competent authorities and judges, in the presence of the conditions laid down, to request evidence from companies on the design, functioning and effects of digital commercial practices on consumer behaviour, in compliance with the principles of necessity and proportionality and the protection of trade secrets. The parallel revision of the Regulation on consumer protection cooperation would also give the European Commission direct powers to investigate and sanction certain cross-border infringements, with penalties of up to 6% of annual worldwide turnover.

For companies operating in e-commerce, digital services and the development of AI solutions, the proposal makes it appropriate to start a review of automated business processes, how chatbots are used, recommendation and personalisation systems, contract purchase and renewal mechanisms and the documentation available to prove their correctness. The Digital Fairness Act does not directly amend the AI Act, but completes its framework of protection in terms of commercial practices, also joining the GDPR and the Digital Services Act. The provisions are still the subject of a legislative proposal and will become applicable only after any final approval by the European Parliament and the Council, according to the timetable that will be established by the adopted text.

European Commission – Digital Fairness Act, proposal COM(2026) 1100 final of 11 November 2026.

---

9 November 2026 – AgID: the final Guidelines on artificial intelligence in the PA have been published. Governance, risk management, data protection and controls obligations on the systems adopted.

With Determination no. 169 of 9 November 2026, the Agency for Digital Italy (AgID) adopted the final Guidelines for the adoption of artificial intelligence in the Public Administration, issued according to the procedure provided for in Article 71 of the Digital Administration Code and as part of the Three-Year Plan for Information Technology in the PA 2024-2026.

The document introduces an organic framework of organizational, technical and regulatory compliance requirements that administrations must consider when introducing and using AI systems, even when acquired from external suppliers.

The Guidelines first of all require administrations to define a strategy for AI, consistent with their institutional functions, with the Integrated Plan of Activities and Organization (PIAO) and with the data governance strategy. The strategy must identify objectives, areas of application, resources and transparency measures. Each project must also be accompanied by the identification of requirements, risk assessment and the definition of indicators to measure the effectiveness, reliability and organizational impact of the systems. The approach follows a model of continuous improvement, inspired by the *Plan-Do-Check-Act cycle* and the ISO/IEC 42001 standard, to be applied in a manner proportionate to the characteristics and complexity of the solutions adopted.

In terms of responsibilities, the coordination of AI governance is entrusted to the Digital Transition Officer (RTD) and the related Office, with the involvement of the Data Protection Officer (DPO) and cybersecurity contact persons. Administrations characterized by a particularly intense use of AI can also identify a dedicated Artificial Intelligence Manager. The adoption of procedures to govern the development, use and monitoring of systems is required, while the preparation of a specific code of ethics and conduct is an optional, albeit recommended, measure.

Of particular importance are the obligations on the protection of personal data, IT security and the protection of fundamental rights. Administrations must verify the lawfulness of processing, the quality and origin of data, the methods of use of personal information and any transfers to third countries. They must also carry out the impact assessments required by the GDPR and, in the cases provided for by the AI Act, those on fundamental rights, ensuring adequate human oversight mechanisms. Security must also include AI-specific risks, such as manipulation of training data, attacks on models and unauthorized extraction of information.

The operational implications also directly concern companies that develop or provide AI systems to public administrations. Entities will have to be able to acquire and verify the technical documentation, safety features, operating methods and evidence necessary to demonstrate the compliance of the solutions, including through checks after their introduction. It is therefore essential for administrations and suppliers to clearly define responsibilities, security requirements, surveillance methods, information obligations and verification tools throughout the entire life cycle of the systems.

The Guidelines expressly distinguish between mandatory requirements, prohibitions and recommendations. Their adoption therefore represents an important step towards a structured, documentable and continuously verified governance of AI in the PA, destined to affect both the internal organization and the methods of acquisition and management of technologies.

AgID – Determination no. 169/2026 and Final Guidelines for the adoption of AI in the Public Administration.

---

3 November 2026 - Advocate General of the Court of Justice of the EU: when a chatbot uses press articles to respond to users, it can affect publishers' rights.

In his Opinion in Like *Company v Google Ireland* (C-250/25), Advocate General Maciej Szpunar addresses the use of journalistic articles by chatbots such as Gemini. The focus is on *retrieval-augmented generation* (RAG) response generation: the system retrieves an online publication in real time and uses it to answer the user's question. This activity must be distinguished from the previous training of the model. On the two questions relating to training, the Advocate General proposes that the Court should not rule, considering them hypothetical in the present case because it has not been proven that the publisher's articles were used for that purpose. The observations which it makes in any event concerning the exception to *text and data mining* do not, therefore, constitute the proposed solution to the dispute.

As for the chatbot's responses, Szpunar refers to the related right granted to publishers by Article 15 of Directive (EU) 2019/790. He proposes to assess, among other things, how the system accessed the article — in particular whether it circumvented a paywall or other effective technical measures — and what appears in the response. The publisher's right does not confer a monopoly on news events: a response that reports the same facts with an autonomous formulation is not, for that reason alone, equivalent to the reproduction of the article. It is different if the expressive form of the publication is recognizable in the response to the point of making it unnecessary for the user to read the source. The Advocate General also examines the possible liability of the provider when such uses are inherent in its commercial strategy or are not countered by adequate and effective measures. He does not conclude, however, that the example produced by Like Company already demonstrates a violation: he leaves the investigations on the case to the national judge.

For publishers, this issue makes it important to document content access control measures and to keep verifiable examples of responses generated by AI services, comparing them with original articles. For chatbot providers, it draws attention to the rules given to source retrieval systems, response filters and, where necessary, licensing agreements. However, it is not enough to note that a response reduces traffic to a newspaper to automatically infer a violation of the related right: according to the proposed approach, the concrete methods of access and reuse of the publication must be verified.

Status: Opinion of the Advocate General delivered on 3 November 2026 and non-binding. The Court of Justice has yet to give its ruling.

text of the Opinion, C-250/25, ECLI:EU:C:2026:919 and Court Notice No 155/26 of 3 November 2026.

CYBERSECURITY

6 November 2026 – Department for Digital Transformation: technical specifications adopted to test the IT-Wallet.

The Presidency of the Council of Ministers has made public the decree of the Head of the Department for Digital Transformation adopting the technical specifications of the IT-Wallet System for the experimentation phase. The measure implements the framework set by the decree of 17 June 2026: the guidelines define the system system, while the specifications constitute the detailed reference for developing and verifying the participants' solutions.

For companies and public administrations interested in issuing electronic certificates, offering digital wallets or verifying their content, the transition is operational. It is necessary to identify the role to be assumed and compare architecture, interoperability, security and data processing with the applicable specifications before starting integration and testing. The technical documentation is published by the Department in an open repository, destined to evolve also in the light of the results of the experimentation: those who develop solutions will therefore have to check for updates and distinguish the formally adopted version from subsequent work in progress.

The adoption of the specifications does not equate to the indiscriminate opening of all IT-Wallet services to the public. At this stage, it regulates the technical path of the subjects participating in the experimentation.

At the same time, AgID defined the rules for registering with the IT-Wallet and proposing new use cases. With determination no. 164 of 23 October 2026, published on the same day, AgID adopted version 1.0 of the regulation on registration in the IT-Wallet System and participation in the Experimentation Space. The text distinguishes the roles of participants — including providers of private wallets and certificates, entities that verify certificates, aggregators and holders of authentic sources — and establishes documents and requirements to be submitted according to the planned activity.

While waiting for the *onboarding portal* to be fully operational, the application is submitted with the form attached to the regulation, digitally signed or with a qualified electronic signature by the legal representative and sent via PEC to AgID. The investigation assesses the administrative, organizational and technical requirements; if a denial is not communicated within 90 days, the application is considered accepted with reservations. This step should not be confused with the actual registration in the IT-Wallet Register, which requires passing the technical checks and tests.

The Experimentation Space allows registered entities to validate and integrate their solutions. A separate experimentation project, to be submitted to AgID, is necessary when you want to test functionalities, services or use cases not yet covered by the rules or specifications. For interested companies and PAs, the first activity is therefore to choose the role, prepare the corresponding documentation and assess whether their use case also requires the admission of a project. Participation is voluntary and does not in itself confer a right to funding or to the continuation of the service in ordinary operation.

determination of AgID and attached regulation; AgID press release.

publication of the Presidency of the Council; project page and technical documentation of the Department; decree of 17 June 2026 in the Official Gazette.

---

25 October 2026 – National Agency for Cybersecurity - ACN: simplified NIS 2027 registration for already registered subjects, but only if the data have not changed.

ACN Determination No. 314287/2026, adopted on 20 October to update the procedures for using the NIS platform, has applied since 25 October. The most immediate news concerns the 2027 registration campaign: according to the Agency's communication, entities already on the NIS list do not have to submit a new declaration if they have no changes to communicate with respect to the information already transmitted. The ACN also updated the registration FAQs and announced that, from 31 October 2026, it would no

longer be possible to send late declarations relating to the previous campaign, to allow the platform to be adapted.

Simplification is not equivalent to an exemption from internal controls. Before making use of it, the companies and PAs concerned should compare the previous declaration with the current situation: perimeter of activities and services, organisational data, contact persons and other information communicated to the Agency. If changes have occurred in the meantime, the updating requirements provided for by the NIS regulations must be assessed. It is useful to assign this verification to an internal manager and keep the outcome: the absence of a new declaration must depend on the actual absence of changes, not on a lack of recognition.
The determination updates the platform's procedures; it should not be confused with the ACN acts that govern the security measures required of NIS subjects. Before sending the newsletter, I suggest a final check of the PDF of the act: the ACN website did not allow it to be opened in full during this check, and this news is therefore limited to the points confirmed by the Agency's public communication.

ACN communication on NIS 2027 registration and determination no. 314287/2026.

INFORMATION TECHNOLOGY

10 November 2026 - Campania Regional Administrative Court, Salerno: in online tenders, the upload of documents is not enough to submit the bid.

The reopening of the terms of an online tender is an exceptional remedy: it is not enough for the competitor to report that he or she has not been able to submit the bid. A proven malfunction of the platform or absolute technical uncertainty as to the cause of the failure to submit is required. This is the principle applied by the Campania Regional Administrative Court, Salerno, in judgment no. 1839, published on 27 October 2026.

In the case examined, relating to a tender by the Salerno ASL for home care and telemedicine, the company had uploaded the contents of the offer by the deadline, but without completing its finalization and registration. The technical investigation traced the failure to complete it to the import of a P7M file instead of ZIP in the specific phase in which the platform required the latter format. The system had reported the error before the deadline; the operator's checks had not detected any interruptions or anomalies in the service. The TAR therefore rejected the request to evaluate the offer or to reopen the terms. The issue, the ruling specifies, is not the admissibility in general of the P7M digital signature, but compliance with the technical sequence provided for that operation.

For companies and contracting authorities, the decisive distinction is between *uploaded documents* and *the offer actually transmitted and acquired*. Operators should complete the submission in advance, check the formats required at each step and keep the acquisition receipt; in case of impediment, report it immediately with detailed technical elements. Before deciding on an extension, administrations must carry out and document checks on the functioning of the platform: an individual reinstatement, without the ascertained conditions, risks violating equal treatment between competitors.

DIGITAL MARKETS

5 November 2026 - EU Court of Justice: the smart meter is not optional for the sole fact that the customer prefers a traditional meter.

In its judgment in *Netz Niederösterreich* (C-468/24), in an Austrian dispute, the Court of Justice clarified the scope of the European rules on the introduction of smart meters. Articles 19, 21 and 22 of Directive (EU) 2019/944 do not oblige the network operator to comply with the final customer's request not to receive a smart meter and to install a conventional meter in its place. The directive, therefore, does not grant the

customer a general right to object to the installation. The national provisions applicable to the individual relationship remain to be verified.

The Court also ruled on data security: it is not necessary for all the requirements to be reproduced in the national standard defining the smart meter, provided that they are implemented in the relevant provisions of the legal system. As regards the ePrivacy Directive, the mere transmission of data through an electricity network does not make that network a public electronic communications network to which Article 5(3) on access to information in terminal equipment should therefore apply. This does not exempt consumption data from the rules of the GDPR.

In practice, operators and suppliers should not treat the ruling either as an obligation to always offer an alternative meter, or as an exemption from privacy obligations. The purposes and legal bases of the processing, the granularity of the data collected, the parties authorized to access it, the security of transmissions and the information provided to customers remain to be monitored. The Court, on the other hand, did not resolve the specific issue of the visibility on the meter of early access to consumption data, judging it hypothetical in the procedure examined.

Court of Justice of the EU, judgment of 5 November 2026, C468/24, ECLI:EU:C:2026:936.

INTELLECTUAL AND INDUSTRIAL PROPERTY

4 November 2026 – EU General Court: in short marks, a common word is not enough to demonstrate the likelihood of confusion.

In Case T696/25, SUNS/SUN68, relating to clothing products, the General Court of the European Union partially annulled a decision of the Board of Appeal EUIPO. The Board of Appeal had given the common term 'sun' excessive distinctive weight for some of the goods, underestimating the differences between the signs: the particular graphic representation of SUNS, the final 's' and the number '68' of the earlier mark. According to the General Court, even where the goods are identical, the comparison must take into account the overall impression of the marks and the actual weight of the elements of which they are composed.

The ruling is useful in the choice of new trade names and in the management of oppositions, especially in sectors where evocative or widespread words recur. However, it does not definitively close the dispute: it remains to be examined, among other things, whether the earlier trademark has acquired a greater distinctive capacity through use. For companies, the practical lesson is twofold: a lexical coincidence does not decide the case alone; those who invoke the acquired strength of their trademark must be ready to document it.

Judgment of the General Court of the EU of 4 November 2026, ECLI:EU:T:2026:723.
