

Regulatory update Data protection, AI, IT and IP

No. 19/2026

DATA PROTECTION

13 October 2026 – European Data Protection Board (EDPB): smart glasses require effective transparency even towards passers-by.

12 October 2026 – The Italian Data Protection Authority reminds the deadline of 29 October regarding pixel tracking in emails.

11 October 2026 – Privacy Guarantor: debt collection, the updated version of the vademecum is online. Stop invasive practices such as text messages or pre-recorded phone calls.

ARTIFICIAL INTELLIGENCE

12 October 2026 - AI Act: the first harmonised standard for high-risk AI systems, dedicated to quality management, has been published.

8 October 2026 – AI Act in Italy: Decree 179/2026 defines controls, penalties and rules for the use of AI in companies.

CYBERSECURITY

15 October 2026 – NIS 2: in October the 18-month deadline for the adoption of basic security measures by NIS registered and registered subjects in 2025 expires.

11 October 2026 – European Supervisory Authorities: Q&A clarification on the classification of incidents related to successful malicious accesses.

10 October 2026 - Cyber Resilience Act: ENISA FAQs clarify how to report vulnerabilities and incidents through the single European platform.

DIGITAL MARKETPS

15 October 2026 – EU Court of Justice: in payment services, gross negligence of the customer does not exempt the payment service provider from immediate reimbursement of the amount of an unauthorised payment transaction.

INTELLECTUAL AND INDUSTRIAL PROPERTY

15 October 2026 – WIPO - International trademarks: Saudi Arabia in the Madrid System, it is now possible to designate Saudi territory in registration applications.

8 October 2026 – Trade secrets: the new Art. 98 IPC includes AI data and training methods.

8 October 2026 - EUIPO and the European Banking Federation strengthen cooperation in the financial sector secured by intellectual property.

DATA PROTECTION

13 October 2026 – European Data Protection Board (EDPB): smart glasses require effective transparency even towards passers-by.

The European Data Protection Board (EDPB) adopted a **Statement on smart glasses** on 13 October 2026. These are initial interpretative reflections, not guidelines or guidelines (the Statement does not introduce a general ban on smart glasses). Cameras, microphones, streaming and artificial intelligence functions can acquire data from people who do not use the device and do not perceive that they are being filmed or heard. The EDPB reports accentuated risks in places of care, schools, workplaces and restricted spaces, including for business secrets and intellectual property.

The distribution of roles depends on who decides on the purposes and means: the user, producer and provider of the app or AI function can be independent controllers or joint controllers. The exception for exclusively personal or domestic activities is interpreted strictly: it does not cover professional use or publication on a social profile open to an indeterminate number of people. Furthermore, any exemption of the private user does not exempt the producer and provider from their obligations.

Traditional information aimed at the buyer alone is not sufficient for the third parties filmed. The Committee proposes **visible and difficult-to-deactivate registration signals**, possibly combined with acoustic indicators and other contextual measures. Consent from passers-by collected after filming does not legitimise the collection that has already taken place; legitimate interest requires a concrete balance and is particularly difficult to sustain for commercial reuse and AI training. Minimisation, retention, rights, special data, transfers and, in relevant cases, ePrivacy rules remain to be assessed.

For manufacturers, app providers and companies evaluating the use of the device, data acquisition, real-time support and reuse should be separately mapped, as well as the legal basis and feasibility of transparency towards third parties should be verified, and continuous recording and access to sensitive areas should be restricted.

12 October 2026 – The Italian Data Protection Authority reminds the deadline of 29 October regarding pixel tracking in emails.

The Italian Data Protection Authority recalled that the six-month period granted by the Guidelines of 17 April 2026, published in the Official Gazette on 29 April, expires on 29 October 2026. The October recall makes it urgent for companies, mass sending platforms and newsletter managers who use remote images or equivalent techniques to detect recipients' openings and behaviour to adapt.

According to the Authority, the pixel can fall under art. 122 of the Privacy Code and, for tracking purposes, requires prior, free, specific and informed consent, except for the limited technical, security or institutional and service communication hypotheses contemplated by the Guidelines. The information must explain what is measured, for what purposes and with which subjects; the recipient must be able to withdraw consent easily and in a granular way. The GDPR discipline continues to apply to roles, accountability, minimization and *privacy by design*.

In practice, it is necessary to register the pixels embedded in the templates, the settings of the *marketing providers* and the openings recorded also on behalf of third parties; disable tracking until the valid choice; separate the revocation of tracking from the management of communications, when appropriate; update the information, register and contractual agreements.

Finally, it should be remembered that the Authority has indicated the verification of the Guidelines among the areas of inspection in the Plan for the second half of 2026.

11 October 2026 – Italian Data Protection Authority: debt collection, the updated version of the vademecum is online. Stop invasive practices such as text messages or pre-recorded phone calls.

The new edition of the "[Privacy and debt collection](#)" handbook is online, a practical guide to guide companies specializing in debt collection, banks, financial companies, telephone or energy companies towards full respect for the fundamental rights of citizens, preventing unlawful processing or treatment that is detrimental to the dignity of the person. The document of the Italian Data Protection Authority reiterates – in line with the provisions of the GDPR – the need to balance the creditor's legitimate interest in recovering the sums owed to him and the protection of the debtor's confidentiality.

But let's see in more detail the main clarifications contained in the vademecum.

The legal basis and limits of competence of the Guarantor

The processing of personal data for debt collection purposes is lawful even without the debtor's consent, as it is based on the legitimate interest of the data controller. The Authority specifies, however, that the Authority does not have jurisdiction over disputes relating to the existence or amount of the credit, for which citizens must contact the relevant authorities (e.g., ordinary judicial authorities, Antitrust, Arera).

Illegal and lawful practices

The Authority's investigations have highlighted the persistence of invasive behaviour. In this regard, the Authority recalls that it is forbidden to exert undue pressure or communicate the state of non-compliance to third parties. Visits to the home or at work that expose the debtor's condition, pre-recorded reminder phone calls without an operator (which risk being listened to by third parties), the posting of notices of default on the door of the house or in the condominium hallway, and the sending of mail with visible external writings such as "debt collection" are unlawful.

On the other hand, it is allowed to search for the debtor (even in the workplace), as long as no reference is made to the debt. Postal communications must be in closed envelopes and without writings regarding credit recovery.

The data that the persons in charge may process

The persons in charge may process personal data, tax code, the amount of the credit and the contact details provided in the contract. But also data acquired from public databases, registers or authorized third-party sources.

Accountability and disclosure obligation

Creditors are obliged to carry out periodic checks on the work of external agencies and must provide the debtor with a clear and detailed privacy policy.

ARTIFICIAL INTELLIGENCE

12 October 2026 - AI Act: the first harmonised standard for high-risk AI systems, dedicated to quality management, has been published.

By [Implementing Decision \(EU\) 2026/2274](#) of 12 October 2026, published in the Official Journal of the European Union on 14 October 2026 and which entered into force on the same day, the Commission published the reference to standard EN 18286:2026, 'Artificial intelligence — Quality management system for the purposes of the regulatory requirements of the EU AI Regulation'. The annex to the decision contains, for now, only one standard: it is therefore not the publication of the full set of technical standards expected for high-risk systems.

The standard covers the supplier quality management system under Article 17 of the AI Act. In operational terms, this system must be documented through policies, procedures and instructions covering, among

other things, compliance strategy, system design and modifications, audits and testing, data and risk management, post-market monitoring, incident reporting and the attribution of internal responsibilities. EN 18286:2026 provides suppliers with a common technical reference to organise and make these processes verifiable.

For companies, the first check is to determine whether they take on the role of supplier under the AI Act for one or more systems. If so, it is appropriate to compare the management system already in place with EN 18286:2026, identify missing procedures and records, and document how controls, changes and monitoring are managed.

Those who already have a system based on ISO 9001 or ISO/IEC 42001 can use it as a working basis: the European standard contains correlation tables, but the existence of those certifications is not equivalent, on its own, to demonstrating compliance with the AI Act. The adoption of the standard remains voluntary and does not exhaust the other obligations applicable to high-risk systems.

A legal point to follow: CEN-CENELEC presents the citation in the Journal as the source of a presumption of conformity for the Article 17 quality system. The text of Article 40(1) of the AI Act, however, expressly refers to the requirements of *Section 2* of the Chapter on high-risk systems, while Article 17 is placed in *Section 3*. It is therefore prudent to verify the precise scope of the presumption before describing EN 18286:2026 as an automatic proof of compliance with the whole of Article 17. Its officially published technical reference value remains unchanged.

8 October 2026 – AI Act in Italy: Decree 179/2026 defines controls, penalties and rules for the use of AI in companies.

Legislative [Decree No. 179 of 7 October 2026](#), published in the Official Gazette No. 234 of 8 October 2026 and applicable from 23 October 2026, adds – after the rules of Legislative Decree 160/2026 – new rules to the Italian regulatory framework on AI (Law 132/2025 and delegated decrees).

Who supervises and how. The decree assigns **AgID** the task of evaluating, designating and monitoring the bodies that, in the cases provided for by the AI Act, verify the compliance of AI systems. **ACN**, on the other hand, entrusts market supervision: checking compliance with the rules applicable to AI systems and intervening in the event of violations. For high-risk systems used in their respective financial areas, supervision is the responsibility of the **Bank of Italy, CONSOB and IVASS**; the powers of the Privacy Guarantor on AI and biometrics in high-risk systems remain unaffected. The text regulates control powers, corrective measures and complaints: a company that develops or uses AI will therefore have to identify the competent authority based on the system and sector, prepare verifiable documentation and know who will handle a possible dispute. Complaints submitted to the wrong authority will be automatically forwarded to the competent authority. In certain cases in the financial sector, customer disputes relating to infringements of the AI Act may be dealt with by existing out-of-court resolution bodies, within the limits of their competence.

Personnel decisions: effective human control. Article 41 is among the provisions with the greatest immediate impact for employers. If an AI system intervenes in the processes relating to the establishment, modification or termination of the relationship, including performance evaluations and disciplinary decisions, the final decision cannot be based solely on automated processing: it must be taken by a person exercising **effective and autonomous** power. The employee's consent does not remove this constraint. The decree excludes from this specific provision the search and selection of candidates, even when a person does not access the next phase; however, the other relevant rules, including those of the GDPR, remain applicable. Before processing, the employer must comply with the information obligations referred to in Article 41. Upon request, the worker can obtain, with the intervention of a person, a comprehensible justification for the decision, indicating the possible weight of the AI and the main parameters considered. Decisions taken in violation of the prohibition of paragraph 1 are **null and void**, including dismissal. In practice, a mere formal approval of the output of the system does not offer the guarantee of autonomous human judgment: it is necessary to organize and be able to reconstruct the decision-making process.

Health and safety. Article 42 requires the use of AI that affects the organisation of work, production rhythms, methods of performance or safety-relevant decisions to be assessed, as part of the risk assessment provided for by Legislative Decree 81/2008. Employers must also inform and train workers on specific risks and prevention and protection measures. For example, before introducing tools that assign tasks, change rhythms or assist operational decisions, it will be appropriate to involve HR and safety functions in the assessment of concrete effects on work.

Penalties and management of disputes. Article 23 provides for differentiated ceilings: up to **€35 million or, if higher, 7% of annual worldwide turnover** for practices prohibited by the AI Act; up to **€15 million or 3%** for violations of the European obligations listed in the provision; up to **€7.5 million or 1%** for inaccurate, incomplete or misleading information provided to authorities or notified bodies. There is a specific range, up to **1 million or 0.5%**, for violations of Articles 27 and 86 of the AI Act. For SMEs, micro-enterprises and innovative start-ups, the determination criterion referred to in Article 99(6) of the Regulation applies. These amounts are **ceilings**, not automatic sanctions: the verification must be carried out on the provision infringed, its date of application and the circumstances of the case.

Experimentation and protection of technological assets. The decree establishes an Italian regulatory experimentation space for AI (so-called *regulatory sandbox*), jointly managed by AgID and ACN, with a focus on access by SMEs and start-ups. However, the operating procedures and admission criteria require further measures: the establishment of the space is not yet equivalent to the opening of applications. On the industrial property front, Article 52 clarifies that data, algorithms, model architectures and training methods can only fall under the protection of trade secrets **if** they meet the ordinary requirements of secrecy, economic value deriving from secrecy and reasonable protection measures. For AI developers, this makes it particularly important to document accesses, confidentiality agreements and technical protection measures.

Companies can start by reconnaissance of the AI systems used in HR processes, in activities that affect safety and in regulated services; for each, it is advisable to record the purpose, the role of the company, the supplier, the potentially competent authority, the expected human intervention and the documentation available. It is a concrete basis for adapting procedures and contracts without assuming that all systems fall under the same obligations or deadlines.

CYBERSECURITY

15 October 2026 – NIS 2: in October the 18-month deadline for the adoption of basic security measures by NIS registered and registered subjects in 2025 expires.

For organizations included in the NIS list during 2025, **the adoption of basic security measures expires 18 months after receipt of the notification of inclusion**. ACN reports that the first deadlines fall in October 2026, but the exact day must be obtained from the notification received from each entity: there is no single date in October valid for everyone. The framework derives from the determinations on the basic specifications and ACN clarifications; [the vademecum of 11 September 2026](#) is an operational tool, not a new postponement of the deadline.

Adoption requires the concrete implementation of the requirements applicable to important or essential subjects, with documentary evidence, risk assessment, procedures and involvement of the administrative and management bodies. It is advisable to close the gaps identified in the technical audits, track decisions and responsibilities, align contracts and supplier oversight, and separately verify the incident notification procedures already in place. The mere formal approval of a policy does not demonstrate the implementation of the technical and organizational requirements.

The timetable differs for those who first entered **the list in 2026**: basic measures are due by **31 July 2027**, and the notification of basic significant incidents starts from **1 January 2027**, according to ACN determination 127434/2026.

11 October 2026 – European Supervisory Authorities: Q&A on DORA to clarify the classification of incidents related to successful malicious accesses.

Q&A 2026_7779, published as definitive in the *Single Rulebook* of the European Supervisory Authorities (EBA, ESMA and EIOPA), interprets Art. 6, letter c), of Delegated Regulation (EU) 2024/1772 on the DORA regulatory framework on the classification of ICT incidents. Successful, malicious and unauthorised access to a financial entity's network and information systems must be assessed independently for the purposes of the "*criticality of the services concerned*", **even if the compromised systems do not support critical or important functions** and even if the access passed through the network of an ICT third-party provider.

The clarification prevents *triage* from ruling out an incident just because a system deemed non-critical has been affected or because the initial vector is at the supplier. However, it does not mean that every intrusion is automatically a **major incident**: the overall classification requires the application of the thresholds and other criteria of the delegated regulation.

For banks, insurance companies and other DORA entities, it is useful to update the SOC Playbooks and incident classification procedures, providing for documented verification of successful access and severity criteria even in vendor compromise scenarios. Contracts and *escalation* flows with ICT third parties should make available in time the logs and facts necessary for the assessment and any notifications.

10 October 2026 - Cyber Resilience Act: ENISA FAQs clarify how to report vulnerabilities and incidents through the single European platform.

In [the FAQ updated on 3 October 2026](#), ENISA specifies how to use the Single Reporting Platform, operational since 11 September. Manufacturers of products with digital elements must use it to report actively exploited vulnerabilities and serious incidents affecting product safety: a first alert must be sent within 24 hours of becoming aware of the event and a more complete notification within 72 hours, in both cases without undue delay. A single notification is sufficient even if the manufacturer has several companies or offices in the EU, but the relevant coordinating CSIRT must be selected.

ENISA warns that, in the current version, the platform's 72-hour counter may indicate an inaccurate deadline, because it calculates 48 hours from the sending of the first notice. The company must therefore independently keep track of when it became aware of the event. Voluntary notifications are not yet available on the platform; the corresponding obligations for *open-source software stewards* will apply from 11 December 2027

DIGITAL MARKETS

15 October 2026 – EU Court of Justice: in payment services, gross negligence of the customer does not exempt the payment service provider from immediate reimbursement of the amount of an unauthorised payment transaction.

The payment service provider may, however, subsequently claim reimbursement from the customer of losses resulting from gross negligence on the part of the customer. A customer of a Polish bank was the victim of *phishing* fraud: a third party presented himself as interested in purchasing an item that she was selling on an online sales platform and sent her a fraudulent link, presented as originating from that platform and intended to confirm the sale. Deceived, she clicked on that link which led to a website that resembled that of her bank and entered her connection details to the e-banking service. Thanks to that data, the third party in question was able to transfer an amount of approximately EUR 700 from the customer's bank account to an account in his name. The following day, the customer reported the fraudulent transaction to her bank. However, the customer refused to refund the amount of the unauthorised payment transaction, taking the view that the customer, through gross negligence, had made that transaction possible and failed to fulfil its obligation to protect the personalised security credentials. Following this refusal, the customer brought an action before a Polish court, which asked the Court of Justice of the European Union whether, in the light of EU law, the bank, as a payment service provider, is obliged to immediately reimburse the amount of an unauthorised transaction, even if it considers that the customer has committed gross negligence.

In its judgment, the Court answers in the affirmative. In the event of an unauthorised payment transaction, the payment service provider is, in principle, required to reimburse the amount of that transaction immediately, at the latest by the end of the first business day following that on which it became aware of or was informed thereof, provided that the customer informs that payment service provider thereof without delay.

There is only one exception to this immediate reimbursement obligation: where the payment service provider has reasonable grounds to suspect fraud committed by the customer and notifies the competent national authority of those reasons in writing. The fact that the payment service provider considers that the customer made the unauthorised transaction possible due to gross negligence – in particular by failing to take the necessary measures to protect the personalised security credentials – does not allow it to refuse immediate reimbursement. Indeed, EU law makes it possible to distinguish between the question of the reimbursement of the amount of the unauthorised payment transaction and that of who is ultimately to bear the losses relating to that transaction. Therefore, as a first step, the payment service provider is required to make the immediate reimbursement. Subsequently, it may, where appropriate, claim reimbursement from the customer of the losses incurred if it proves that those losses arise from the fact that the customer, intentionally or through gross negligence, has breached its obligations, in particular the obligation to protect personalised security credentials. It is for the payment service provider to prove the existence of such gross negligence on the part of the customer.

INTELLECTUAL AND INDUSTRIAL PROPERTY

15 October 2026 – WIPO - International trademarks: Saudi Arabia in the Madrid System, it is now possible to designate Saudi territory in registration applications.

The Madrid Protocol entered into force for Saudi Arabia on 8 October 2026. Italian companies using the Madrid System can now apply for protection in the country through a new international application or a subsequent designation of an existing registration.

For those who export or intend to enter the Saudi market, it is time to check their portfolio, classes and storage strategy.

The accession was announced by WIPO on **July 23**; the novelty of the period considered is its **entry into force**.

The [official WIPO notice](#) specifies, among other things, that the ordinary time limit for notifying a provisional refusal is **18 months** and that an individual fee applies.

8 October 2026 – Trade secrets: the new Art. 98 IPC includes AI data and training methods.

Art. 52 of Legislative Decree 179/2026, published on 8 October and effective from 23 October 2026, adds paragraph 1-bis to art. 98 of the Industrial Property Code. Company information and technical-industrial experience that can be protected may include **data, algorithms and mathematical methods for training AI systems**, including model architectures, optimization functions, training procedures and configurations.

The standard does not attribute automatic protection to every dataset or algorithm. However, the three conditions already provided for by art. 98, paragraph 1 must be met: secret information, the economic value of secrecy and reasonably adequate measures to maintain it. Coordination with licenses, copyright, Data Act and GDPR remains necessary: the qualification as a trade secret does not authorize unlawful processing of personal data or allow legal access obligations to be evaded.

For companies that develop or commission AI models, it is advisable to inventory datasets, pipelines, weights and configurations that are effectively confidential, define access by role, marking and logging, confidentiality agreements and rules for suppliers and employees. In a dispute, the proof of the protection measures taken will be as central as the description of the technical asset.

8 October 2026 - EUIPO and the European Banking Federation strengthen cooperation in the financial sector secured by intellectual property.

The European Union Intellectual Property Office (EUIPO) and the European Banking Federation (EBF) have signed a Memorandum of Understanding to strengthen cooperation at the intersection of intellectual property, finance and business support. The agreement combines the EUIPO's expertise in intellectual property with practical experience and knowledge of the European banking sector, represented through the EBF's network of national banking associations. The EBF brings together 33 national banking associations as full members and 10 associate members across Europe, representing around 3,500 banks.

Joint efforts will focus on strengthening the financial recognition of intellectual property rights, expanding commercial lending capacity against intangible assets, and integrating long-term collaboration between both ecosystems.

For many innovative companies, some of their most valuable assets are intangible, from technology and designs to trademarks and other forms of intellectual property. However, assessing their value, applicability, and potential recovery remains a challenge for financial institutions. Closer cooperation between intellectual property experts and the banking sector can help fill these information gaps and improve understanding of how those assets can be taken into account in financing decisions.

Earlier this year, the EUIPO published [IP-backed finance in Europe: State of Play and Future Perspectives](#), identifying structural barriers to the wider use of intellectual property in accessing finance, including challenges related to disclosure, assessment, data and risk assessment.

The study was followed by the [European Roadmap for IP-Supported Finance](#), developed through cooperation with EU institutions, national intellectual property offices, financial institutions, businesses and experts. The agreement with the EBF represents another practical step in this ongoing effort to bring the intellectual property and financial communities closer together.

[The agreement](#) provides a framework for continued cooperation, with specific activities to be developed through joint work plans.