

Regulatory update Data protection, AI, IT and IP

No. 18/2026

DATA PROTECTION

21 September 2026 – EDPB: Guidelines 3/2025 on the interplay between DSA and GDPR definitively adopted.

19 September 2026 – EDPB Guidelines 04/2026: when supervisory authorities should impose gdpr administrative fines and when other corrective measures may apply.

ARTIFICIAL INTELLIGENCE

15 September 2026 – Artificial Intelligence and liability: legislative decree no. 160/2026 introduces new obligations and risks for businesses.

CYBERSECURITY

13 September 2026 – Italian National Cybersecurity Agency: NIS handbook now available online.

11 September 2026 – European Commission: Cyber Resilience Act – operational guidance published; first reporting obligations apply from 11 September.

INFORMATION TECHNOLOGY

17 September 2026 – EU Commission: EU Kids Act, new rules on age verification, safety by design and online protection of minors.

12 September 2026 – Data Act: “access by design” requirements for data generated by connected products apply from 12 September 2026.

DIGITAL MARKETS

19 September 2026 – European Bank Authority - EBA: new guidelines on third-party risk management for non-ICT services adopted.

INTELLECTUAL AND INDUSTRIAL PROPERTY

18 September 2026 – Court of Justice of the European Union: even a short social media post may qualify as a copyright-protected work.



18 September 2026 – Court of Justice of the European Union: even a short social media post may qualify as a copyright-protected work.

DATA PROTECTION

21 September 2026 – EDPB: Guidelines 3/2025 on the interplay between DSA and GDPR definitively adopted.

EDPB adopted the final version of the **Guidelines 3/2025 on the interplay between the Digital Services Act and the GDPR**, clarifying how the two Regulations must be coordinated where compliance with obligations under the **Digital Services Act (DSA)** entails the processing of personal data.

The underlying principle is particularly relevant for businesses: **the DSA does not replace the GDPR and does not, in itself, constitute a general legal basis for the processing of personal data**. Any processing carried out in the context of DSA compliance must therefore be assessed independently under the GDPR, including by identifying the applicable legal basis and verifying necessity, proportionality, data minimisation, transparency, data protection by design, the potential applicability of Article 22 on automated decision-making, and the need to conduct a DPIA.

The Guidelines focus in particular on a number of areas with significant operational implications.

With regard to **content moderation**, the EDPB distinguishes between voluntary activities and processing that is necessary to comply with specific legal obligations. Voluntary activities aimed at detecting illegal content may, where the relevant conditions are met, be based on legitimate interests; where, by contrast, the processing is required by a specific legal obligation, Article 6(1)(c) GDPR may apply. The EDPB nevertheless makes clear that the DSA cannot justify generalised monitoring or profiling of users. Where automated content moderation results in the removal of content or the suspension of accounts, the potential applicability of Article 22 GDPR must also be assessed, and any human intervention must be genuine and effective rather than merely formal.

In relation to **online advertising**, the EDPB clarifies that the transparency obligations laid down by the DSA are additional to, and do not replace, those arising under the GDPR. The DSA obligation to inform users about the parameters used for advertising does not provide an autonomous legal basis for targeting. Of particular importance is also the prohibition on using **special categories of personal data**, including such data inferred through profiling, for advertising based on profiling: the prohibition applies even where the processing might, in principle, be permitted under Article 9 GDPR.

As regards **recommender systems**, the EDPB stresses that, where the DSA requires the availability of an option that is not based on profiling, that choice must also be effective from a technical perspective. Merely displaying a different feed is not sufficient: where the user selects the non-profiled option, the provider should not continue to collect or use personal data in order to profile that user for future recommendations. In certain circumstances, moreover, an automated recommendation may amount to a decision falling within the scope of Article 22 GDPR, for example in services that recommend job vacancies or real-estate opportunities.

The Guidelines also devote particular attention to **dark patterns**, clarifying that, where manipulative design affects choices concerning the processing of personal data, the GDPR principle of fairness becomes directly applicable. Interfaces that induce users to provide more data, accept less privacy-protective options or engage in compulsive behaviours may therefore be relevant simultaneously under both the DSA and the GDPR.

Further guidance concerns the **protection of minors**. The EDPB acknowledges that DSA obligations may justify age-assurance processing, but emphasises the need for proportionate and privacy-preserving solutions. Platforms should avoid the generalised collection of identity documents or the use of other mechanisms resulting in the unique identification of users where this is not strictly necessary and, where possible, should limit themselves to verifying whether or not the relevant age threshold has been met.

For businesses, the operational message is clear: **DSA and GDPR compliance can no longer be managed through separate compliance programmes**. Content moderation, advertising, recommender systems, complaint handling, the protection of minors and systemic risk assessments must be analysed

jointly, by linking each DSA obligation to the data-processing activities required to implement it and verifying their compliance with the GDPR.

Businesses should therefore consider putting in place an **integrated DSA-GDPR compliance matrix**, capable of mapping, for each process, the purposes of processing, legal basis, categories of data, retention periods, any automated decision-making, security measures and the need for a DPIA. It is precisely this integration between the digital-law obligation and the underlying processing activity that the EDPB now places at the centre of compliance.

19 September 2026 – EDPB Guidelines 04/2026: when supervisory authorities should impose gdpr administrative fines and when other corrective measures may apply.

The European Data Protection Board (EDPB) has adopted the new **Guidelines 04/2026 on the exercise of the power to impose administrative fines in relation to the other corrective powers provided for under the GDPR**, which were subsequently published for public consultation from **21 September to 13 November 2026**.

The document addresses an issue that is distinct from the mere calculation of the amount of fines: it clarifies **when a Data Protection Authority should impose an administrative fine and when, instead, it may rely on other corrective powers** under Article 58(2) GDPR, such as warnings, reprimands, orders to bring processing operations into compliance, restrictions or bans on processing, and the withdrawal of certifications. On this point, the new Guidelines replace the previous guidance of the Article 29 Working Party and complement the **Guidelines 04/2022**, which concern the methodology for calculating the amount of administrative fines.

The objective is to promote greater consistency in enforcement across the European Union through a **five-step methodology**.

First, the Supervisory Authority must verify that the infringement identified is in fact punishable by an administrative fine under the GDPR or, where permitted, under national law. It must then determine **which entity may be held liable** – for example, the controller, processor, certification body or monitoring body – and establish that the infringement was committed **intentionally or negligently**. Only after completing these preliminary assessments does the Authority consider, on the basis of the criteria laid down in Article 83(2) GDPR, whether the infringement may be classified as “minor” and, finally, whether the imposition of an administrative fine would be **effective, proportionate and dissuasive** in the circumstances of the particular case.

Of particular relevance to businesses is the clarification concerning **corporate liability**. Referring to the case law of the Court of Justice, the EDPB states that controllers and processors may be held directly liable for infringements committed by directors, employees or other persons acting within the scope of the organisation’s activities and on its behalf: **it is not necessary to establish that the management body was aware of the conduct, nor is it necessarily required to identify the individual natural person to whom the infringement may materially be attributed**.

The Guidelines also devote particular attention to the requirement of **fault**. At least negligent conduct must be established before an administrative fine may be imposed, but the threshold identified by the EDPB is relatively low: the relevant question is whether the entity **was in a position to be aware of the unlawfulness of its conduct and ought to have been aware of it had it exercised the ordinary degree of diligence required in the circumstances**. Mere ignorance of the applicable legal framework is therefore not sufficient to exclude negligence.

Nor does the existence of an **internal or external legal opinion** automatically have exculpatory effect. Among the examples set out in the Guidelines, the EDPB considers that negligence may still be established where an undertaking has followed legal advice that departs from settled or well-known guidance issued by the Supervisory Authority or from established legal doctrine; similarly, undocumented external advice, or advice based on incomplete information, is not in itself sufficient to exclude liability.

A central part of the Guidelines concerns the distinction between **minor and non-minor infringements**. The Supervisory Authority must carry out an overall assessment of the aggravating and mitigating factors referred to in Article 83(2), taking into account, inter alia, the nature, gravity and duration of the infringement, the number of data subjects affected, the damage suffered, the degree of fault, the measures taken to mitigate the consequences, previous infringements, the degree of cooperation with the Authority, the categories of data concerned and any financial benefits obtained.

Where an infringement is classified as **minor**, the general rule identified by the EDPB is that no administrative fine should be imposed and that another corrective measure, such as a reprimand, may instead be appropriate. This is not, however, an automatic rule: depending on the specific circumstances, a fine may still be imposed for a minor infringement. Conversely, where the infringement is **not minor**, the Guidelines identify a strong presumption – and, in general terms, the rule – in favour of imposing an administrative fine, without prejudice to the Authority's ability to decide otherwise where required by the principles of effectiveness, proportionality and dissuasiveness. In exceptional circumstances, it may even be unnecessary to exercise any corrective power at all.

The EDPB further emphasises that **compliance measures already required under the GDPR do not automatically qualify as mitigating factors**. When assessing the degree of responsibility, the Authority will instead consider whether the controller or processor did what could reasonably be expected in light of the nature, purposes and scale of the processing, and whether the measures implemented under Articles 24, 25 and 32 GDPR effectively reduced the residual risks to data subjects.

The **conduct adopted after the infringement** is also relevant. Prompt mitigation of the damage, effective cooperation with the Supervisory Authority and the voluntary adoption of measures capable of preventing recurrence may influence the overall assessment. Conversely, the existence of previous infringements – particularly infringements of the same type – or the repetition of conduct initially capable of being classified as minor may reveal a systemic organisational deficiency and make the imposition of a fine more likely.

From an operational perspective, the Guidelines 04/2026 therefore reinforce the importance of **effective and demonstrable GDPR compliance**. For businesses, it becomes particularly important to be able to demonstrate not only the formal existence of policies and procedures, but also the effective implementation of accountability measures; to retain evidence of legal assessments and decisions taken; to document the consideration and implementation of the DPO's recommendations; to maintain procedures for the prompt remediation of infringements; and to monitor any previous incidents or recurring compliance weaknesses that could cause isolated events to be regarded as evidence of structural organisational shortcomings.

The new Guidelines therefore complete the EDPB's framework on administrative fines: **the Guidelines 04/2022 explain how the amount of a fine should be calculated, whereas the Guidelines 04/2026 address when such a fine should be imposed in relation to the other corrective measures available to Supervisory Authorities**.

ARTIFICIAL INTELLIGENCE

15 September 2026 – Artificial Intelligence and liability: legislative decree no. 160/2026 introduces new obligations and risks for businesses.

On **15 September 2026**, **Legislative Decree No. 160 of 9 September 2026** was published in the Italian Official Gazette, General Series No. 214. The Decree is entitled "Adaptation of national legislation to the provisions of Regulation (EU) 2024/1689 [...] concerning the use of artificial intelligence systems for law-enforcement activities and civil and criminal liability". The Decree will enter into force on **30 September 2026**.

The measure represents one of the main domestic legislative steps taken to implement and complement the European regulatory framework on artificial intelligence and gives effect to the delegation of legislative powers contained in **Law No. 132 of 23 September 2025**. Its significance, however, is not confined to public security authorities: alongside rules governing the use of AI by law-enforcement authorities, the

Decree introduces provisions of general application concerning **criminal liability, the administrative liability of legal entities under Legislative Decree No. 231/2001, and compensation for damage caused through the use of artificial intelligence systems.**

For businesses, therefore, the publication of Legislative Decree No. 160/2026 marks a particularly significant step in the evolution of the **AI Act from a framework primarily focused on regulatory compliance into a body of rules capable of producing consequences also in the fields of civil and criminal liability.**

The Decree consists of **22 Articles divided into three Titles. Title I (Articles 1-10)** governs the use of AI systems in law-enforcement activities, including research and testing, training, human oversight, biometric-data processing, real-time remote biometric identification and post-remote facial recognition.

Title II (Articles 11-20) addresses criminal and civil liability: it introduces Article 437-bis of the Criminal Code, regulates the procedural use of biometric identification, amends the rules governing seizure of online content generated also through AI, introduces the new Article 25-vicies into Legislative Decree No. 231/2001 and establishes specific rules governing claims for damages relating to AI systems.

Title III (Articles 21-22) contains transitional and financial provisions; AI systems already covered by contracts or already being developed, tested or used in law-enforcement activities are granted a one-year period to comply with the provisions of Chapter II of Title I.

Legislative Decree No. 160/2026 makes clear that compliance with the AI Act should be integrated into a broader **enterprise risk-management** framework. Businesses concerned should assess, in particular, the classification of the AI systems they use and whether any qualify as high-risk systems; the adequacy of security measures and human-oversight arrangements; the retention of logs and technical documentation capable of serving an evidentiary function; the updating of risk mapping and organisational models under Legislative Decree No. 231/2001; internal procedures governing the creation and dissemination of synthetic content; liability and indemnity provisions in contracts with providers and suppliers; and the adequacy of insurance coverage in light of the new liability scenarios.

The most significant systemic development is that **compliance and liability are becoming increasingly interconnected.** Compliance with the AI Act remains essential, but is not, in itself, sufficient to exclude civil liability; conversely, breaches of the obligations imposed by the EU Regulation may directly affect the evidentiary framework, while certain conduct relating to the security of high-risk systems may give rise to criminal liability and, where the statutory conditions are met, to the liability of the entity under Legislative Decree No. 231/2001.

For businesses, AI governance must therefore increasingly be integrated with **Legislative Decree No. 231/2001 compliance, cybersecurity, product safety, litigation management and insurance coverage**, moving beyond an approach confined to formal compliance with the AI Act.

CYBERSECURITY

13 September 2026 – Italian National Cybersecurity Agency: NIS handbook now available online.

The plenary meeting of the National Cybersecurity Agency's [NIS](<https://www.acn.gov.it/portale/nis>) Implementation Working Group, attended by the sectoral authorities and regional representatives, examined in greater detail the determinations adopted by the Director General of ACN. An update of the list of NIS entities was ordered, covering more than 2,000 late registrations and approximately 2,000 review proceedings examined by ACN between May and July. This activity forms part of the collaborative implementation process pursued by ACN in its capacity as the national NIS authority, with a view to ensuring effective oversight of the country's productive system.

A consultation on strengthened security measures has also been launched. The measures have been developed in accordance with the principles of proportionality and gradual implementation underpinning the NIS framework. The consultation process, conducted ****through the sectoral working groups****, is

intended to supplement and replace the baseline security measures adopted during the initial implementation phase of the NIS Decree.

This is the third consultation through which the Agency, together with the sectoral authorities, has invited constructive engagement with the sectors concerned regarding the implementing measures under the NIS Decree. Contributions received will be taken into account during the Authority's review process, in accordance with the principle of participatory regulation that characterizes ACN's approach.

The Working Group also recalled that the new registration or update window for public and private entities falling within the scope of the NIS framework will open on 1 January 2027. Registration will close on 28 February 2027.

Since mid-September, the [NIS Handbook](#) has also been available, providing general guidance on the main compliance obligations and related deadlines, as well as specific guidance on selected topics. The first upcoming deadline, in October, concerns the implementation of the baseline security measures by entities included in the NIS list in 2025.

The next deadline concerns registration for 2027. As in each year, from 1st January to 28 February all NIS entities are required to complete or update their online registration by accessing ACN's services portal. The specific guidance also addresses the updating of information and the categorization of activities and services.

Registration, in addition to being a mandatory compliance requirement, is the first step towards becoming part of the community of NIS entities and gaining access to the support activities provided by ACN and CSIRT Italia within a framework of participatory regulation and cooperative compliance.

By updating its information, a NIS entity shares with the competent national NIS authority (ACN) the information required under the NIS Decree, thereby enhancing the protection of the entity's networks and information systems, as well as those of the country as a whole, including through strengthened analyses aimed at safeguarding the systemic relevance of the supply chain.

Through the categorization of activities and services, NIS entity also carries out a simplified impact assessment based on a harmonized model and shares the outcome with ACN, in order to determine proportionate obligations concerning security measures.

11 September 2026 – European Commission: Cyber Resilience Act – operational guidance published; first reporting obligations apply from 11 September.

From **11 September 2026**, one of the first sets of substantive obligations under **Regulation (EU) 2024/2847 – the Cyber Resilience Act (CRA)** has become applicable: manufacturers of products with digital elements are now required to report **actively exploited vulnerabilities** and **severe incidents having an impact on the security of their products**, in accordance with the timelines and procedures laid down in Article 14 of the Regulation. At the same time, ENISA has made the **CRA Single Reporting Platform (SRP)** operational as the single EU reporting point through which such notifications must be submitted.

This marks a particularly significant stage in the CRA's phased implementation. The Regulation entered into force on 10 December 2024 and will become fully applicable on **11 December 2027**. However, the EU legislature brought forward the application of certain provisions: following the rules concerning conformity assessment bodies, applicable from 11 June 2026, the **Article 14 reporting obligations** have applied since 11 September 2026.

The new requirements directly concern **manufacturers of products with digital elements**, broadly meaning entities that place on the Union market, under their own name or trademark, hardware or software products featuring a direct or indirect logical or physical connection to a device or network. The scope is therefore extremely broad and includes IoT devices, connected equipment, software, applications,

operating systems, hardware and software components, industrial devices and numerous other categories of digital products.

A particularly important point is that **the reporting obligations also apply to products with digital elements already made available on the Union market before 11 December 2027**. Businesses should therefore not assume that they may wait until the CRA becomes fully applicable before adapting their vulnerability and incident management procedures: the Article 14 reporting regime is already in force.

Which events must be reported

The CRA distinguishes between two categories of events subject to mandatory reporting.

The first consists of “**actively exploited vulnerabilities**”. The mere existence of a vulnerability, or the fact that it could theoretically be exploited, is therefore insufficient. Under the Regulation, a vulnerability is considered actively exploited where there is **reliable evidence that a malicious actor has exploited it in a system without the permission of the system owner**.

The second category concerns **severe incidents having an impact on the security of a product with digital elements**. An incident is considered severe where it negatively affects, or is capable of negatively affecting, the ability of the product to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or where it has led, or is capable of leading, to the introduction or execution of malicious code in the product or in the network and information systems of one of its users.

This distinction is also important from an operational perspective: **not every vulnerability is subject to mandatory reporting under Article 14**; the requirements for “active exploitation” must be met. Similarly, not every security anomaly or event will automatically qualify as a “severe incident”. Businesses must therefore be capable of rapidly assessing and classifying events against the definitions set out in the Regulation.

Reporting is subject to particularly stringent deadlines. The CRA establishes a sequence of successive notifications.

For an **actively exploited vulnerability**, the manufacturer must submit:

-
- an **early warning within 24 hours** of becoming aware of the vulnerability;
 - a **vulnerability notification within 72 hours**, including, where available, general information concerning the affected product, the nature of the exploit and vulnerability, the corrective or mitigating measures already taken, and the measures that users may take;
 - a **final report within 14 days after a corrective or mitigating measure becomes available**, including at least a description of the vulnerability, its severity and impact, any available information concerning the malicious actor, and details of the security update or other corrective measures made available.
-

For **severe incidents**, the manufacturer must instead submit:

-
- an **early warning within 24 hours** of becoming aware of the incident, indicating at least whether the incident is suspected of being caused by unlawful or malicious acts;
 - an **incident notification within 72 hours**, including, where available, information on the nature of the incident, an initial assessment and any corrective or mitigating measures taken;
 - a **final report within one month of the 72-hour notification**, providing a detailed description of the incident, its severity and impact, the likely type of threat or root cause, and the mitigation measures adopted or still underway.
-

INFORMATION TECHNOLOGY

17 September 2026 – EU Commission: EU Kids Act, new rules on age verification, safety by design and online protection of minors.

On 17 September 2026, the European Commission presented its proposal for a Regulation, the **EU KIDS Act – “EU Keeping Internet Digital Spaces Accountable and Trustworthy” (COM(2026) 681 final)**, aimed at strengthening and harmonising the protection of minors when using digital services across the European Union. At this stage, the initiative remains a legislative proposal, which must be considered by the European Parliament and the Council and may therefore be amended during the legislative process.

The proposed framework goes well beyond the highly visible issue of establishing a minimum age for access to social media. It introduces a graduated access regime: **children under the age of 13 would not be permitted to hold social media accounts; users aged 13 to 14 could access social media only through restricted accounts subject to parental or guardian supervision; from the age of 15, minors would be allowed to open and manage their accounts independently.** Accounts held by 13- and 14-year-olds would be subject, among other requirements, to permanent parental-control mechanisms and a daily usage limit not exceeding one hour. Within six months from the date on which the new rules become applicable, the platforms concerned would also be required to verify existing accounts and disable those attributable to users under the age of 15, or where the user’s age cannot be established in accordance with the prescribed procedures.

Of particular significance for businesses is the principle of **“safety by design”**. Providers would no longer be able to rely solely on ex post control mechanisms; instead, they would be required to design services and functionalities with the risks to minors taken into account from the outset. Subject to differentiated obligations, the proposed rules would apply not only to social networks and video-sharing platforms, but also to **online video games, app stores, AI companions and conversational chatbots**. Measures identified by the Commission include restrictions on design techniques capable of encouraging compulsive use — such as infinite scrolling, continuous autoplay, certain types of notifications and “streak” mechanisms — together with more protective default settings, restrictions on contact by unknown users and specific requirements concerning recommender systems used in services accessed by minors.

A further key area concerns **age verification**. A mere self-declaration of the user’s date of birth would no longer be sufficient in the situations governed by the Regulation. The proposal instead envisages the use of certified age-assurance mechanisms, including the European age-verification solution and, subsequently, the European Digital Identity Wallet. At the same time, the architecture outlined by the Commission seeks to reconcile age verification with the data-minimisation principle: through “zero-knowledge proof” techniques, the service should be able to establish only whether the user is above or below a specified age threshold, without receiving the user’s identity or any additional personal data. The future framework will therefore also need to be interpreted and implemented in conjunction with the **GDPR**, as well as with the obligations already arising under the Digital Services Act.

Specific provisions are also envisaged for **artificial intelligence systems intended for, or accessible to, minors**. AI companions and chatbots should not use interaction techniques capable of creating emotional dependency through the simulation of human relationships. In addition, certain functionalities would have to be disabled by default, while providers would be required to assess risks to minors before making the system available and to monitor such risks thereafter. In this respect, the KIDS Act establishes a direct interface with the governance and supervisory framework laid down by the **AI Act**.

The proposed enforcement regime is also particularly stringent. For the largest platforms, the model outlined by the Commission would effectively require them to **demonstrate compliance before enabling interactions involving minors**: VLOPs would be required to prepare a detailed compliance plan and submit it to independent verification. The sanctions contemplated by the proposal may reach **up to 6% of total worldwide annual turnover**, relying, in respect of platforms and AI systems, on the supervisory structures already established under the DSA and the AI Act respectively.

From an operational perspective, the proposal already warrants close attention from businesses that design or provide digital services that may be used by minors. In particular, companies should assess whether their services are likely to fall within the future scope of application, map functionalities that depend on knowing or estimating a user's age, review recommender systems, notifications, engagement mechanisms and in-app purchases, and consider the future integration of age-assurance and parental-control tools. Providers of AI systems will also need to coordinate this analysis with the classification and compliance requirements already arising under the AI Act; for all operators, the design of age-verification mechanisms will need to be accompanied by a specific assessment of the associated data-protection implications.

The proposal therefore does not merely introduce an “EU age threshold” for social media. Rather, it anticipates a broader regulatory model under which **the protection of minors becomes a structural requirement in the design of digital products and services.** Businesses potentially affected should therefore monitor the legislative process closely, particularly as regards service design, data governance and the interaction between the compliance obligations arising under the KIDS Act, the DSA, the GDPR and the AI Act.

12 September 2026 – Data Act: “access by design” requirements for data generated by connected products apply from 12 September 2026.

A new phase relates the application of **Regulation (EU) 2023/2854 – the Data Act**: from **12 September 2026**, the obligation laid down in Article 3(1) will apply, requiring connected products and related services placed on the market after that date to be designed so as to enable users to access data generated through their use. The provision applies throughout the European Union and is therefore also relevant to manufacturers and service providers marketing products or services on the Italian market.

The Data Act has applied, as a whole, since **12 September 2025**. Until now, however, the user's right to obtain data generated through the use of a connected product may, in certain circumstances, require a specific request to the data holder. With this new phase of application, the EU legislature takes a further step towards an **“access by design”** model: data accessibility must be built into the design of the product or service itself, rather than being managed solely through subsequent request procedures.

More specifically, Article 3(1) of the Data Act provides that **connected products must be designed and manufactured, and related services must be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely and free of charge accessible to the user in a comprehensive, structured, commonly used and machine-readable format.** Where relevant and technically feasible, access must also be **direct**.

The rules apply to a very broad range of **Internet of Things (IoT)** devices. The concept of a connected product includes, for example, **smartwatches and health-monitoring devices, smart-home equipment, connected cars and other vehicles, industrial and agricultural machinery, and other devices capable of collecting or generating data concerning their use or environment and communicating such data electronically.** “Related services” are also covered, including applications, software or remote-monitoring services connected to the product and necessary for its operation or capable of affecting its functionalities.

The data concerned generally include **raw and pre-processed data generated by the use of the connected product or related service that are readily available to the data holder**, together with the relevant metadata. Depending on the product, this may include data concerning temperature, pressure, location, speed, acceleration, use or equipment performance. By contrast, data inferred or derived through additional processing and protected content are, in principle, outside the scope of Chapter II, without prejudice to the specific provisions of the Regulation and to intellectual property law.

“Access by design” does not, however, mean that every item of data must necessarily be stored physically on the device or that direct access is required in every case. Article 3 requires direct access only where **relevant and technically feasible**. Where users cannot access the data directly from the product or related service, the mechanism laid down in Article 4 of the Data Act continues to apply, under which the

data holder must make the relevant data and metadata available to the user, upon simple request and without undue delay, free of charge and, where relevant and technically feasible, continuously and in real time.

The right is not limited to consumers. For the purposes of the Data Act, users may also include **businesses that own, rent or lease a connected product** or receive a related service. The new regime is therefore particularly significant in **B2B relationships**, for example in relation to industrial machinery, vehicle fleets, professional devices and IoT equipment, enabling business users to exploit the data generated for maintenance, process optimisation, performance analysis or the use of aftermarket service providers other than the original manufacturer.

The requirement to make data accessible to users is closely linked to another central objective of the Data Act: enabling users to **use the data themselves and make them available to third parties of their choice**, thereby fostering the development of maintenance, repair and other data-driven services and reducing lock-in to the original manufacturer.

From an operational perspective, this new phase of application requires manufacturers and service providers to carry out a compliance assessment that cannot be limited to contractual documentation. Businesses should verify whether products and services placed on the market after 12 September 2026 fall within the definitions of “connected product” and “related service”; identify which data and metadata fall within the scope of the Data Act; assess whether the technical architecture enables direct user access; implement appropriate interfaces, dashboards, applications, APIs or other technical solutions; and adequately document the reasons why direct access may not be technically feasible in specific cases. The CCPC itself recommends that data holders carry out this assessment and be able to demonstrate and document the reasons for any absence of direct access.

Compliance must also be coordinated with requirements concerning **security, trade secrets, intellectual property and personal data protection**. The Data Act applies to both personal and non-personal data, but does not alter the lawfulness requirements laid down by the GDPR: where the requested data include personal data relating to individuals other than the user, their disclosure must in any event be supported by a valid legal basis under data protection law.

The 12 September 2026 deadline therefore marks a significant step in the implementation of the Data Act: **access to data generated by connected products must no longer be treated merely as a right to be handled ex post, but as a requirement to be embedded in the architecture of the product and related service from the design stage onwards.** For manufacturers, IoT providers and providers of related digital services, compliance with the Data Act is therefore becoming a matter of product design, data architecture and technical governance, in addition to contractual compliance.

DIGITAL MARKETS

19 September 2026 – European Bank Authority - EBA: new guidelines on third-party risk management for non-ICT services adopted.

The European Banking Authority (EBA) has published its new **Guidelines on the management of risks arising from third-party providers of non-ICT services (EBA/GL/2026/09)**. The Guidelines are final, but are not yet applicable: their date of application will be determined at a later stage.

The initiative marks a shift from a regulatory framework focused on **outsourcing** towards a broader model of **third-party risk management**. Once applicable, the new Guidelines will replace the EBA’s 2019 Guidelines on outsourcing arrangements and will complement the framework introduced by **DORA**, which instead governs risks associated with ICT third-party service providers.

The new framework is based on the principle of **proportionality** and imposes the most stringent requirements on arrangements with third parties supporting **critical or important functions**, namely functions whose disruption could materially affect the financial entity’s operations or its ability to comply with applicable regulatory requirements.

The Guidelines adopt a lifecycle-based approach to the relationship with the service provider, covering **pre-contractual risk assessment, provider due diligence, contractual arrangements, management of subcontracting, ongoing monitoring, documentation and exit strategies**.

A key principle remains unchanged: **the use of a third party does not transfer to the provider the regulated entity's responsibility for compliance with its own obligations**. Particular attention must therefore be paid to the quality of due diligence, oversight and audit rights, the management of subcontracting chains, and the ability to terminate the relationship without jeopardising operational continuity.

The entities concerned will also be required to maintain a **structured mapping of their third-party arrangements**, identifying those that support critical or important functions and coordinating this framework with the controls already required under DORA for ICT third-party service providers.

A **two-year transitional period** is provided for the adaptation of existing arrangements, running from the future date of application of the Guidelines.

From an operational perspective, financial-sector entities should therefore begin reviewing their governance of non-ICT third-party providers, including the inventory of existing arrangements, risk-assessment criteria, contractual provisions, subcontracting arrangements, oversight and audit rights, operational continuity arrangements and exit strategies.

The most significant development is the gradual move away from a fragmented approach to outsourcing: **third-party risk is becoming a distinct area of governance, to be managed in an integrated manner throughout the entire lifecycle of the relationship**.

INTELLECTUAL AND INDUSTRIAL PROPERTY

18 September 2026 – Court of Justice of the European Union: even a short social media post may qualify as a copyright-protected work.

The Court of Justice of the European Union, in **Case C-598/24, Gândul Media Network**, laid down important principles and provided significant guidance on the copyright protection of content published on social media platforms.

The dispute concerned a text of only **22 lines posted on Facebook** by a Romanian teacher and subsequently reproduced in full, without prior authorisation, on the website of an online newspaper.

The Court clarified that **the brevity of the text, the informal nature of the publication and the fact that the content was disseminated through a social media platform do not, in themselves, preclude copyright protection**. What matters is whether the text constitutes the author's own intellectual creation, reflecting free and creative choices, for example in the selection, arrangement and combination of words. It is for the national court to carry out that assessment in the specific case.

The Court also addressed the **exception for reporting current events** laid down in Article 5(3)(c) of Directive 2001/29. Member States may limit that exception to the reproduction of short extracts, provided that such a restriction is proportionate and does not undermine the purpose of the exception. Reproduction of a work in its entirety may therefore go beyond what is justified by the informational purpose pursued, unless, for example, the brevity of the work would make partial reproduction unreasonable.

The Court nevertheless ruled out the possibility of excluding the exception as a matter of principle solely because the reproduction generates an **economic or commercial advantage**: journalistic activity is itself normally carried out professionally and in the context of an economic activity. The use must, however, remain justified by the informational purpose and comply with the other requirements laid down by copyright law.

For businesses, publishers, communications agencies and marketing departments, the practical implication is significant: **the fact that content is publicly available on social media does not mean that it**

may be freely reused. Before reproducing posts, texts or other online content in full, organisations should assess both whether the material may be protected by copyright and whether a specific copyright exception or limitation is actually applicable.

18 September 2026 – Court of Justice of the European Union: even a short social media post may qualify as a copyright-protected work.

The Court of Justice of the European Union, in **Case C-598/24, Gândul Media Network**, laid down important principles and provided significant guidance on the copyright protection of content published on social media platforms.

The dispute concerned a text of only **22 lines posted on Facebook** by a Romanian teacher and subsequently reproduced in full, without prior authorisation, on the website of an online newspaper.

The Court clarified that **the brevity of the text, the informal nature of the publication and the fact that the content was disseminated through a social media platform do not, in themselves, preclude copyright protection.** What matters is whether the text constitutes the author's own intellectual creation, reflecting free and creative choices, for example in the selection, arrangement and combination of words. It is for the national court to carry out that assessment in the specific case.

The Court also addressed the **exception for reporting current events** laid down in Article 5(3)(c) of Directive 2001/29. Member States may limit that exception to the reproduction of short extracts, provided that such a restriction is proportionate and does not undermine the purpose of the exception. Reproduction of a work in its entirety may therefore go beyond what is justified by the informational purpose pursued, unless, for example, the brevity of the work would make partial reproduction unreasonable.

The Court nevertheless ruled out the possibility of excluding the exception as a matter of principle solely because the reproduction generates an **economic or commercial advantage**: journalistic activity is itself normally carried out professionally and in the context of an economic activity. The use must, however, remain justified by the informational purpose and comply with the other requirements laid down by copyright law.

For businesses, publishers, communications agencies and marketing departments, the practical implication is significant: **the fact that content is publicly available on social media does not mean that it may be freely reused.** Before reproducing posts, texts or other online content in full, organisations should assess both whether the material may be protected by copyright and whether a specific copyright exception or limitation is actually applicable.
