Weinhold Legal

Digital Legal Update

JANUARY 2026

Below, we bring you the latest updates from the digital sector. Should you have any questions regarding the matters outlined below, please do not hesitate to contact us.

Contents

LEGISLATIVE NEWS

Cybersecurity Act

The new Cybersecurity Act (Act No. 264/2025 Coll.), which implements the NIS2 Directive, entered into force on 1 November 2025.

At the same time, its implementing regulations also came into effect, in particular the following decrees issued by the National Cyber and Information Security Agency (NÚKIB):

- Decree No. 334/2025 Coll. on the Portal of the National Cyber and Information Security Agency and requirements for certain procedures,
- Decree No. 408/2025 Coll. on regulated services,
- Decree No. 409/2025 Coll. on security measures for providers of regulated services under the higher obligations regime,
- Decree No. 410/2025 Coll. on security measures for providers of regulated services under the lower obligations regime.

Providers of regulated services were required to notify the relevant regulated services by 31 December 2025.

Critical Infrastructure Resilience Act

The new Act No. 266/2025 Coll., on the Resilience of Critical Infrastructure Entities (the Critical Infrastructure Act), transposes Directive (EU) 2022/2557 on the resilience of critical entities (the CER – Critical Entities Resilience Directive). **The Act entered into force on 19 August 2025**.

The system of critical infrastructure is not a new concept; it has been embedded in the Czech legal framework since 2010, specifically in the Crisis Management Act.

Weinhold Legal

Digital Legal Update

JANUARY 2026

Previously, the legislation focused on elements of critical infrastructure, i.e. assets, buildings, facilities, or networks designated by the competent authorities.

Under the new approach, the focus has shifted to the provision of an essential service by a given operator. Instead of identifying "elements of critical infrastructure," the law now designates **"critical infrastructure entities,"** which subsequently define for themselves the critical infrastructure necessary for the provision of the essential service.

The new Act defines what constitutes an essential service, including, for example, energy supply, healthcare, transport, water management, digital infrastructure, or the functioning of public administration.

An essential service provider is any entity that provides such a service within the territory of the Czech Republic and at the same time meets at least one of the significance criteria, such as the number of users, market share, or the dependence of other sectors on the service.

An essential service provider that commenced the provision of an essential service no later than 30 November 2025 is required to submit relevant information to the competent authorities **by 1 March 2026**. However, the implementing legislation has not yet been adopted, namely:

- a Government Regulation on essential services and significance criteria,
- a decree on the requirements for and processing of the resilience plan, risk assessment, and the content of measures to ensure the resilience of critical infrastructure entities,
- a decree specifying the details of incident reporting in relation to critical infrastructure entities, and
- a decree on the Critical Infrastructure Portal.

PROPOSED LEGISLATION

Digital Omnibus

On 19 November 2025, the European Commission presented a new legislative package entitled **Digital Omnibus**. The main objective of this package is **to simplify regulation and reduce administrative burdens**. Digital Omnibus primarily affects the Digital Services Act (DSA), Digital Markets Act (DMA), AI Act, Data Governance Act, Data Act, and, to a more limited extent, also the GDPR and ePrivacy framework.

Digital Services Act

With regard to the DSA, the Digital Omnibus does not alter the substantive obligations of platforms or liability for illegal content. Instead, it focuses on the procedural and institutional alignment of the DSA's enforcement with other EU digital regulations, in particular the GDPR, AI Act, DMA, and Data Act. The aim is to increase legal certainty and predictability of supervision, reduce duplicative proceedings and uncoordinated sanctions, and clarify the allocation of competences among supervisory authorities, without weakening or simplifying the substantive obligations arising from the DSA.

AI Act

Relief measures are proposed for companies that develop or use artificial intelligence systems. Under the original rules of the regulation known as the AI Act, companies are required to register certain high-risk AI systems in an EU database. The new proposal seeks to abolish this obligation for systems that formally fall within the high-risk category but do not, in practice, pose a significant risk to fundamental rights (for

example, systems designed solely for narrow procedural tasks). Instead of registration, companies would only be required to prepare their own internal assessment and retain it for potential supervisory review.

The proposed changes also affect education and training. The AI Act introduced an obligation for operators and providers of AI systems (including employers) to ensure AI literacy, i.e. the ability to understand how AI systems function. Digital Omnibus proposes to shift primary responsibility for this obligation to the Member States and the European Commission, which should ensure appropriate awareness-raising and tools.

In addition, EU-wide AI "sandboxes" are planned from 2028, enabling developers to test AI systems safely in real-world environments without the risk of immediate sanctions.

GDPR

In the area of personal data protection, the proposal aims to enhance legal certainty and predictability for developers and operators of digital technologies, in particular by clarifying the relationship between the GDPR and other EU digital legislation and by promoting a more consistent application across the EU.

The proposal does not change the rules for determining a legal basis under the GDPR. However, it clarifies that legitimate interest pursuant to Article 6(1)(f) GDPR may, under certain circumstances, be considered a relevant legal basis for the training of AI models or for scientific research, provided that the proportionality test is met and appropriate safeguards are implemented, such as pseudonymisation or purpose limitation. The proposal thus reinforces a risk - based and contextual approach, rather than broadly expanding the use of personal data.

Cookies

A notable change for both users and website operators is the planned limitation of pop-up consent banners for cookies. In addition, cookies that do not pose a risk to users' privacy (such as those used for basic traffic measurement or essential website functionality) would no longer require user consent.

NIS2

In the area of incident reporting, the rules are expected to be harmonised. Currently, companies are required to report a single incident to multiple authorities under different legal frameworks (GDPR, NIS2, DORA). Under the proposed changes, a single contact point for all incident reporting should be established.

Data Act

With regard to the Data Act, the Digital Omnibus focuses on clarifying and coordinating its application with other EU digital legislation, in particular the GDPR, DSA and AI Act. The objective is to enhance legal certainty for entities subject to the Data Act, reduce duplicative notification and supervisory obligations, clarify procedures for public sector data requests, and align the roles of supervisory authorities, without limiting the core obligation to share data in cases provided for under the Regulation.

European Business Wallet

Another key development is the introduction of the **European Business Wallet**. This will be a digital tool enabling companies to easily prove their identity and verify business partners across the EU, with the aim of accelerating and securing cross-border business activities.

The entire legislative package is currently at the **proposal stage** within the European Commission, which has also

Weinhold Legal

Digital Legal Update

JANUARY 2026

launched a public consultation known as the **"Digital Fitness Check."** The consultation will run until March 2026, and **the final shape of the rules may therefore still change**.

Implementation of the AI Act in the Czech Republic

The Ministry of Industry and Trade has prepared a draft Act on Artificial Intelligence.

As EU legislation is directly applicable, the national act does not introduce new substantive rules for the operation of AI systems. Instead, it takes a minimalist approach, focusing solely on the necessary procedural and institutional arrangements that fall within the competence of the Member States.

The Ministry of Industry and Trade will act as the main coordinating authority, while market surveillance and the role of the single contact point will be performed by the Czech Telecommunication Office. The Czech National Bank and the Office for Personal Data Protection will also be involved, while the Office for Technical Standardization, Metrology and State Testing will assume the role of the notifying authority and will accredit conformity assessment bodies. In the area of the protection of fundamental rights, a significant role will be played by the Public Defender of Rights. At the same time, the establishment of a national regulatory sandbox is envisaged, enabling companies to safely test AI systems prior to their placement on the market and to create an appropriate environment for the designation of notified bodies responsible for the certification of selected artificial intelligence systems.

The draft further defines administrative offences and sets out the procedure for imposing sanctions for breaches of the rules. The maximum level of fines is derived directly from the EU Regulation and may reach up to EUR 35 million or 7% of the undertaking's worldwide annual turnover.

The interministerial consultation procedure has been completed, and the individual comments are currently being processed.

Chat Control

On 27 November 2025, the Council of the EU approved its negotiating position on the proposed **CSAM Regulation** (sometimes referred to as "chat control"), which aims to protect children in the digital environment and combat online child sexual abuse. The proposal requires providers of digital services to assess the risks of misuse of their services and, in justified cases, to implement measures to mitigate such risks, including the detection and reporting of illegal content..

The possibility of automated content detection, which in extreme cases could lead to interference with private communications and pressure to weaken end-to-end encryption, has sparked significant controversy. The Council of the EU has therefore sought to find a compromise that would allow for child protection without leading to blanket monitoring of communications. Nevertheless, the proposal remains politically sensitive, and some Member States, including the Czech Republic, continue to oppose solutions that could result in widespread content monitoring or the weakening of encrypted services.

Weinhold Legal

Digital Legal Update

JANUARY 2026

GDPR DEVELOPMENTS

New procedural regulation for cross-border data protection complaints

On 12 December 2025, a new EU procedural regulation was published with the aim of accelerating and streamlining the enforcement of the GDPR in cross-border cases. The previous system for handling cross-border complaints often resulted in lengthy and opaque proceedings, increasing both costs and legal uncertainty for organisations and individuals alike.

A key element is the harmonisation of admissibility criteria for complaints across Member States and the strengthening of the procedural rights of the parties, including the right to comment on key evidence and preliminary findings.

The Regulation sets binding deadlines for the handling of cross-border cases, including a 15-month timeframe, with the possibility of a one-off extension of up to 12 months in exceptionally complex cases. It also introduces an "early resolution" mechanism, allowing proceedings to be closed where the infringement has been remedied and the complaint has become moot, while preserving procedural safeguards for the complainant.

The new procedural rules will become fully applicable as of 2 April 2027.

DMA and GDPR – Joint Guidelines of the EDPB and the Commission

On 9 October 2025, the European Data Protection Board (EDPB) and the European Commission published joint guidelines clarifying obligations under the Digital Markets Act (DMA) and the GDPR.

The purpose of the guidelines is to ensure a consistent interpretation of both instruments and to provide legal certainty for so-called gatekeepers (large digital platforms such as Meta, Google and Apple), which are required to comply with the DMA while at the same time respecting the principles of the GDPR. A key message of the joint guidelines is that both regulations apply in parallel, and that the DMA does not replace the GDPR nor does it introduce a new legal basis for the processing of personal data.

The main topics addressed by the guidelines include:

- requirements for valid user consent under Article 5(2) DMA and the GDPR, enabling gatekeepers to lawfully combine or cross-use personal data across core platform services;
- the obligation to offer a "less personalised but equivalent" version of the service;
- the determination of legal bases for processing and their limitations;
- interoperability (the obligation for gatekeepers to technically enable the interconnection of their services with others) and the requirement to carry out data protection impact assessments (DPIAs);
- coordination of supervision between the European Commission and national supervisory authorities.

The joint guidelines confirm that the DMA and the GDPR complement rather than replace each other, and that the protection of personal data remains a non-negotiable boundary, even in the context of compliance with digital regulation.

The guidelines have been published as a draft for consultation, with comments accepted until 4 December

Weinhold Legal

Digital Legal Update

JANUARY 2026

2025. The final version is expected to be published in 2026.

EDPB Opinion on the Adequacy of the UK

In October 2025, the EDPB adopted two opinions on the European Commission's proposal to extend the UK adequacy decisions (under the GDPR and the Law Enforcement Directive – LED). The Commission proposes to extend the validity of the adequacy decisions for a further six years, i.e. until **27 December 2031**.

The EDPB concluded that the UK legal framework continues, in essence, to be aligned with the EU framework and that personal data may therefore continue to be transferred without the need for additional safeguards. At the same time, however, it identified several areas in which future developments in UK law should be **closely monitored**. These include in particular the new UK test for transfers of personal data to third countries based on the criterion that the level of protection must not be **"materially lower"**, a more permissive approach to automated decision-making and potential limitations on the right to human review, as well as the expansion of exemptions from certain data protection principles in the context of national security and law enforcement. The Commission will need to take these aspects into account in its final decision and ensure their consistent and ongoing monitoring.

Coordinated Enforcement Action 2026

The EDPB has selected compliance with transparency and information obligations towards data subjects as the topic of its fifth coordinated enforcement action, which will take place in 2026.

Supervisory authorities in the individual Member States will focus on assessing whether controllers comply with the requirements set out in Articles 12, 13 and 14 GDPR, and whether they properly inform individuals about the processing of their personal data.

The results of the national investigations will subsequently be aggregated into a joint report, which may serve as a basis for further targeted enforcement measures. This action forms a key part of the EDPB's long-term strategy for 2024–2027 and follows previous coordinated actions focusing on the use of cloud services by the public sector, the role of data protection officers, the right of access, and the currently ongoing assessment of the right to erasure.

EDPS Guidelines on AI Risk Management

On 11 November 2025, the European Data Protection Supervisor (EDPS) issued new guidelines on the identification and mitigation of risks associated with the development, procurement and operation of artificial intelligence systems. The primary objective of these guidelines is to help identify and mitigate risks to individuals' fundamental rights arising from the processing of personal data through AI systems. The guidelines focus on technical measures to ensure compliance with key data protection principles, namely fairness, accuracy, data minimisation and security.

The EDPS emphasises the importance of the interpretability and explainability of AI systems as a prerequisite for meeting other legal obligations and highlights the heightened risks associated with the use of so-called black-box models. In relation to fairness, the guidelines address the elimination of bias arising both from data and from algorithm design,

which may lead to discriminatory outcomes. With regard to accuracy, the EDPS draws attention, inter alia, to hallucinations in generative models and to the risk of data drift (i.e. the degradation of data quality over time). A significant part of the guidelines is also devoted to security threats, including model inversion attacks (where training data can be reconstructed from model outputs), as well as the practical difficulties associated with the exercise of data subject rights.

The guidelines shift the focus from formal GDPR compliance to active and continuous risk management of AI systems. In practice, this means that the deployment of artificial intelligence is not a one-off step, but a continuous process requiring systematic documentation, technical controls and regular assessments of impacts on fundamental rights. Controllers must assess explainability, data quality, security and the practical enforceability of data subject rights already at the stage of selecting or procuring AI systems, ensure these requirements contractually and technically, and continuously monitor risks such as hallucinations, bias or data drift. Responsibility for compliance with legal requirements remains with the controller at all times, not with the AI provider.

EUROPEAN CASE LAW

Relationship between the GDPR and ePrivacy

In its judgment of 13 November 2025 in Case C-654/23, the Court of Justice of the European Union addressed a dispute between a Romanian company operating a legal news website and the Romanian national data protection supervisory authority. The case concerned whether the operator was entitled to send a daily email newsletter to users with a free account without their explicit consent, relying on the "soft opt-in" exemption under the ePrivacy Directive, and without the need to rely on a separate legal basis under the GDPR.

The company argued that user registration constituted a form of sale of a service, which entitled it to send offers of similar services without requiring specific consent. The Court of Justice agreed with the company and confirmed that, in the digital environment, the concept of a sale does not necessarily involve the exchange of money. Where a user registers in order to gain access to content that would otherwise be unavailable, a contractual relationship is formed with the company. The user's email address is therefore obtained in **connection with the sale of a product or service**, as the sending of such an informational newsletter constitutes the use of electronic mail for the purposes of **direct marketing of the controller's own similar products or services**.

Accordingly, the operator may rely on its entitlement to send unsolicited communications relating to its own similar products or services (the so-called soft opt-in) without obtaining separate consent, provided that customers are given a simple and free means to object. Where the specific conditions set out in Article 13(2) of Directive 2002/58/EC (the ePrivacy Directive), which acts as a lex specialis, are met, the general lawfulness requirements under Article 6(1) GDPR do not apply to such processing.

Definition of Pseudonymisation

In its judgment of 4 September 2025 in Case C-413/23 P, the Court of Justice of the European Union ruled in a dispute between the European Data Protection Supervisor (EDPS) and the Single Resolution Board (the "Board") concerning the resolution of the Spanish bank Banco Popular.

The core issue was whether pseudonymised comments submitted by shareholders and creditors of the bank remained personal data after being transferred to an external consultant, where that recipient had no reasonably available means of re-identifying the individuals concerned, and whether information obligations towards data subjects therefore applied in relation to that transfer.

In the case at hand, before transmitting the data to its external consultant, the Board replaced the names of the individuals concerned with numerical codes, i.e. carried out pseudonymisation, as a result of which the consultant was unable to identify the individuals.

The Court of Justice concluded that the pseudonymised comments transmitted to the external consultant did not constitute personal data for that recipient, provided that it had no reasonably available means of identifying the data subjects. However, the Court emphasised that the data remained personal data for the Board itself, as it held the re - identification key. The Board was therefore not required to comply with information obligations in relation to the mere transfer of the pseudonymised data to the consultant; nevertheless, its data protection obligations as the original controller were not affected, and it was required to inform data subjects about the transfer of personal data in accordance with Articles 13 and 14 GDPR.

FURTHER UPDATES

Commission fines X for breach of the DSA

The European Commission imposed a fine of EUR 120 million on Company X for breaches of its obligations under the Digital Services Act (DSA). In particular, Company X infringed the obligations applicable to very large online platforms in the areas of systemic risk management, transparency of service operation, and the handling of illegal and harmful content. The Commission concluded that Company X had failed to adopt sufficient and proportionate measures to protect users and public discourse, as required by the DSA.

The case is significant in that it confirms the practical enforceability of the DSA and demonstrates that platform obligations are not merely formal in nature. The Commission assessed not only the existence of internal rules, but also their actual effectiveness in practice. The decision sends a strong signal to other large online platforms that inadequate risk management, non-transparent algorithms or insufficient content oversight may lead to substantial EU-level sanctions.

This is the first non-compliance decision under the DSA.

Commission: Possible anti-competitive conduct by SAP

The Commission has reached a preliminary view that SAP may have restricted competition in the market for the maintenance and support of on-premise enterprise resource planning (ERP) software.

SAP may have abused its dominant position (in the EEA market for after-sales maintenance and support services for SAP on-premise ERP software) by:

a) imposing an **“all-or-nothing” policy**, requiring customers to source maintenance and support for all of their SAP on-premise ERP software at the same level of support;
b) preventing customers from terminating maintenance and support services for unused software licences

("**shelfware**");

c) extending the initial licence validity period for on - premise ERP software during which maintenance and support cannot be terminated;

d) charging reinstatement and back-maintenance fees to customers who re-subscribe to SAP maintenance and support after a period of absence.

SAP has offered commitments (while not agreeing with the Commission's preliminary assessment):

Key elements of the commitments include:

a) **All-or-nothing policy**: SAP customers may request the unbundling of their digital environment integrating all SAP on-premise ERP software products and licences into separate commercial installations. For each commercial installation, customers will be able to choose different maintenance and support providers and/or different levels of SAP support, or to leave certain installations without support.

b) **Shelfware**: SAP commits to offering greater transparency and broader access to single-metric contracts, under which licence fees – including maintenance and support fees – are calculated based on an agreed metric (e.g. revenue). In addition, customers will be able to create separate commercial installations including shelfware and terminate maintenance and support for such installations.

c) **Extension of the initial validity period**: SAP commits to clarifying its contractual provisions on the extension of the initial validity period and not requiring it to restart upon each additional licence purchase.

d) **Back-maintenance and reinstatement fees**: SAP commits to abolishing reinstatement fees and to reducing back-maintenance fees to 50% of the maintenance and support fees that the customer would have paid had support not been terminated, capped at six months. SAP also commits to fully waiving back-maintenance fees for a list of products no longer supported by SAP and not covered by cross-product licences.

The Commission intends to accept these commitments.

Czech Competition Authority investigates possible abuse of dominance in online job advertising

The Office for the Protection of Competition (ÚOHS) investigated possible abuse of a dominant position by companies within the Alma Career group on the Czech market for online job advertising services.

The Alma Career group operates the best-known Czech job portals jobs.cz and prace.cz, while at the same time acting as a provider of recruitment management software (so-called ATS systems).

The Authority investigated suspicions that the Alma Career group was abusing its privileged market position by creating pricing and technical barriers that made it more difficult to integrate competing ATS solutions and competing job portals with Alma Career's systems.

The administrative proceedings were terminated after the party to the proceedings submitted commitments designed to ensure interoperability with competing services offered on the relevant markets.

© 2026 Weinhold Legal
All rights reserved

Weinhold Legal

Digital Legal Update

JANUARY 2026

The information contained in this bulletin is presented based on our best beliefs and knowledge at the time this text was sent to press. However, specific information relating to the topics covered in this bulletin should be consulted before any decisions are made based on it. The information contained in this bulletin should not be construed as an exhaustive description of the relevant issues and all possible consequences, and should not be relied upon in any decision-making process or considered a substitute for specific legal advice relevant to the particular circumstances. Weinhold Legal, s.r.o. law firm and any lawyer listed as the author of this information are not liable for any damage that may arise from reliance on the information published here. We would also like to note that there may be different legal opinions on some of the issues discussed in this bulletin due to the ambiguity of the relevant provisions, and that in the future, an interpretation other than the one we have presented may prevail.

For further information, please contact the partner/manager with whom you are usually in contact.

Automatic extraction of texts and data, as well as reproduction or extraction of their content for the purposes of automated analysis from this information material, is permitted within the meaning of Article 4 of Directive 2019/ 790/EU and Section 39c of Act No. 121/2000 Coll., the Copyright Act, is permitted if the authorship of Weinhold Legal, s.r.o. law firm is indicated, together with a reference to the location of such text and data.

Martin Lukáš
Partner
martin.lukas@weinholdlegal.com

Tereza Hošková
Vedoucí advokátka
tereza.hoskova@weinholdlegal.com

Nikola Faltová
Advokátka
nikola.faltova@weinholdlegal.com

Jana Duchoňová
Advokátka
jana.duchonova@weinholdlegal.com