Weinhold Legal

Digital Legal Update

SPRING 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

- Critical Infrastructure – Updates
- GDPR Updates
- Proposal for a revised Cybersecurity Act (CSA2)
- Digital Networks Act - návrh Aktu o digitálních sítích
- Proposal for a Civil Code Amendment – Directive on Liability for Defective Products
- CS3D and CSRD – Simplification of Requirements
- Guidelines on the Regulation of Foreign Subsidies (FSR)

Critical Infrastructure – Updates

Providers of essential services which commenced the provision of an essential service by **30 November 2025** at the latest were required to submit information on the essential service and their critical infrastructure to their competent authority for the first time by **1 March 2026**.

In order for providers of essential services to fulfil this obligation, it is necessary for the implementing legislation to enter into force, in particular the **Government Regulation on Essential Services and Significance Criteria**, which, however, has not yet occurred. Providers of essential services are therefore currently unable to assess whether they meet the significance criterion and, consequently, whether they are subject to the information obligation.

The **General Directorate of the Fire Rescue Service of the Czech Republic** has issued a statement on this matter, indicating that providers of essential services must fulfil their information obligation without undue delay after the government regulation enters into force, although the exact date of its effectiveness is still unclear. We will continue to keep you informed of further developments in the legislative process.

You can find our previous summary of the new **Critical Infrastructure Act** here.

GDPR Updates

Annual Report of the Czech Data Protection Authority for 2025

The annual report of the Czech Data Protection Authority (**ÚOOÚ**) for 2025 shows that the authority perceived the past year primarily as a period marked by the strong emergence of new digital regulation and growing demands in terms of methodological, legislative and supervisory activities. In addition to inspections and decision-making practice, the report also highlights the significant methodological and awareness-raising role of the authority — in 2025, the authority received **219 requests for opinions**, issued **168 sets of comments**, and recorded exceptional interest in expert seminars, including a record-attended seminar on **CCTV systems in schools.**

Brazil now "without SCCs": the EU has expanded the map of safe data transfers

On **26 January 2026**, the European Commission adopted an **adequacy decision** in relation to Brazil under **Article 45 GDPR**. In practice, this means that personal data may now be transferred from the European Union to Brazil without

additional specific safeguards, including **standard contractual clauses**, similarly to other countries for which the European Commission has adopted such a decision.

The right to erasure under the GDPR remains a weak spot in corporate practice

In **February of this year**, the **EDPB** published the results of its coordinated enforcement action on the right to erasure and pointed out that the overall level of compliance is only average. The most common issues concern unclear internal processes, deletion of data in backups, poor distinction between erasure and account deletion, and insufficient information provided to data subjects.

Transparency under the GDPR will be another major topic in 2026

The findings of the coordinated enforcement action on the right to erasure were followed in March by the EDPB's launch of a new coordinated enforcement action focusing on transparency and information obligations under the GDPR. This is a clear signal that, in 2026, supervisory authorities will be examining in greater detail how companies explain their processing activities to data subjects and how clearly and effectively they comply with their information obligations.

The dispute over the "simplification of the GDPR" has intensified

In February 2026, the European Data Protection Board (**EDPB**) and the European Data Protection Supervisor (**EDPS**) issued a joint opinion on the proposed **Digital Omnibus**. While they supported the effort to simplify digital regulation, improve the clarity of the rules and reduce unnecessary administrative burden, they also strongly warned against certain proposed amendments to the GDPR. Their strongest criticism was directed at the proposal to change the definition of personal data. According to the EDPB and the EDPS, such a change would not merely constitute a technical clarification, but could substantially narrow the concept of personal data and thereby limit the scope of the GDPR. Both bodies also stated that the proposed wording is inconsistent with the case law of the Court of Justice of the European Union and could lead to greater legal uncertainty rather than genuine simplification.

The EDPB aims to make GDPR compliance easier in practice

In February 2026, the EDPB announced that, as part of its 2026–2027 work programme, it would prepare specific templates and practical materials intended to help organisations comply with the GDPR. These are expected to include, for example, templates for legitimate interest assessments, records of processing activities, privacy notices, personal data breach notifications, and data protection impact assessments.

WhatsApp v EDPB: a direct action may be brought against a binding EDPB decision

In February 2026, the Court of Justice of the European Union ruled that a binding EDPB decision under Article 65 GDPR may, in itself, be subject to judicial review. For companies, this means that in cross-border cases they may challenge an EDPB decision directly, rather than having to wait solely for the final decision of the national supervisory authority.

CJEU: the right of access to personal data has its limits

In its **Brillen Rottler** judgment of **19 March 2026**, the Court of Justice of the European Union confirmed that the data subject's right of access to personal data under Article 15 GDPR is very broad, but not unlimited. A request may exceptionally be considered abusive and the controller may refuse it if it was made solely for the purpose of subsequently

bringing a claim for damages for an alleged GDPR infringement. At the same time, the Court stressed that such a conclusion must be assessed restrictively and that, in order to obtain compensation under Article 82 GDPR, actual damage must be proven.

Regulators continue to impose strict penalties for insufficient personal data security

A notable example from the first quarter of 2026 is the decision of the French supervisory authority, the **CNIL**, which on **13 January 2026** imposed fines totalling **EUR 42 million** on **FREE MOBILE** and **FREE** for failing to ensure an adequate level of security for their customers' personal data. This case once again confirms that supervisory authorities regard technical and organisational security measures, preparedness for security incidents, and the protection of customer data as one of the key areas on which they have long focused in enforcing the GDPR.

Proposal for a revised Cybersecurity Act (CSA2)

On **20 January 2026**, the European Commission proposed a new package of measures focusing on cybersecurity.

Part of this package is the **revised Cybersecurity Act (CSA2)**, which addresses risks in information and communication technology supply chains, in particular risks related to high-risk suppliers from third countries. The main objective of the proposal is to strengthen the cyber resilience of critical infrastructure through a horizontal framework for the security of trusted information and communication technology (**ICT**) supply chains.

The proposal also amends the EU cybersecurity certification framework so that certification schemes would, as a rule, be developed within **12 months**, through a renewed **European Cybersecurity Certification Framework (ECCF)**. These schemes, managed by the **EU Agency for Cybersecurity (ENISA)**, are to become a voluntary tool enabling businesses to demonstrate compliance with EU rules.

At the same time, the package introduces amendments to the **NIS2 Directive** on cybersecurity, aimed primarily at simplifying compliance with the rules and risk management requirements, while also introducing a new category of **small mid-cap enterprises**.

The CSA2 proposal is designed as a complement to the forthcoming **Cloud and AI Development Act (CADA)** and the **Digital Omnibus**.

The Cybersecurity Act itself would become directly applicable immediately upon adoption by the **European Parliament** and the **Council**, while Member States would have **one year from the adoption** of the accompanying amendments to the NIS2 Directive to transpose them into national law.

Digital Networks Act – proposal for a new Digital Networks Act

On **21 January 2026**, the European Commission published a proposal for a **Digital Networks Act (DNA)**, intended to create a new regulatory framework for electronic communications networks and services.

The proposed Digital Networks Act consolidates and amends several existing legal instruments in the field of electronic communications. In particular, it would replace the current **European Electronic Communications Code (EECC)**. It would also replace the **BEREC Regulation**, the **Radio Spectrum Policy Programme (RSPP) Decision**, parts

of the **Open Internet Regulation**, and the **ePrivacy Directive**. A significant new development is that the rules, which were previously governed by directives, are now proposed to be established by regulation.

The European Commission aims to modernize the rules to support the full transition to optical networks, the development of high-quality mobile networks (5G and 6G), as well as the resilience and prosperity of the electronic communications sector. In a broader context, the new regulatory framework is intended to create the foundation for the proper functioning of digital networks and contribute to completing the single market.

The proposal also includes the creation of an **EU Digital Infrastructure Preparedness Plan**. This part of the proposal is interconnected with EU regulations on **cybersecurity**, particularly the **NIS2 Directive** and the EU's **EU-CyCLONE** network for addressing cyber crises.

The **Digital Networks Act (DNA)** will also be closely linked with the upcoming **Cybersecurity Act (CSA2)**. Meeting the conditions set in CSA2 will be one of the requirements for obtaining authorization to operate in the electronic communications sector.

The Commission has published a call for comments on the DNA, with the deadline for submissions set for **20 May 2026**.

Proposal for a Civil Code Amendment – Directive on Liability for Defective Products

Following the **Directive (EU) 2024/2853** of the European Parliament and the Council dated **23 October 2024** on liability for defective products (the "Directive"), the public consultation on the amendment to the Civil Code closed on **26 January 2026**.

Key updates from the Directive and the related amendment to the Civil Code:

The Directive updates the existing EU rules on liability for damage caused by defective products. The definition of "product" is now specifically extended to include software, including all types of applications and artificial intelligence (AI) systems.

The manufacturer will bear **strict liability** for damage:

- that may have occurred after a software update or upgrade carried out under its control;
- arising as a result of the continuous learning of an AI system, as long as the system remains under the manufacturer's control.

The Directive also ensures that there will always be a responsible person in the EU to whom a claim for compensation can be made if the manufacturer is located outside the EU.

Damage

A claim for compensation arises if the defective product caused one of the following types of damage:

- death or personal injury (including psychological damage),
- property damage,
- destruction or damage to data not used for professional purposes.

Previously, only damage exceeding **EUR 500** was compensable; this limitation will now be **removed**.

Limitation Period

Businesses are liable for their defective products for **10 years** from the product's market launch. The **10-year limitation period** is extended to **25 years** if the symptoms of health damage did not appear earlier.

Rebuttable Presumptions

Under the new rules, a product is considered defective if it does not provide the safety that a person is entitled to expect or that is directly required by EU or national law. National courts should presume the defectiveness of a product or the causal link between damage and defect, if it would be too difficult for the claimant to prove the defect or causal link, especially given the technical complexity of the case, even after the defendant has provided information.

Transposition Deadline

The Directive must be transposed into national law by **9 December 2026**, and the new rules will apply to products placed on the market or put into service from that date. Products placed on the market before this date will continue to be governed by the previous regulation.

The draft amendment to the Civil Code also provides for the effectiveness of the law from **9 December 2026.**

CS3D and CSRD – Simplification of Requirements

The **Directive (EU) 2026/470** of the European Parliament and Council, amending Directives **2006/43/EC**, **2013/34/EU**, **(EU) 2022/2464**, and **(EU) 2024/1760** regarding certain corporate sustainability reporting requirements and due diligence requirements in sustainability, was published in the **EU Official Journal** on **26 February 2026**.

This legislation, part of the **Omnibus I** package, aims to simplify the **CSRD** and **CS3D** directives by reducing administrative burdens and limiting the transfer of obligations to smaller suppliers.

The scope of the **CSRD** is narrowed by raising the thresholds to include companies with more than **1,000 employees** and annual net revenue exceeding **EUR 450 million**.

The scope of **CS3D** is also reduced by raising the thresholds to companies with more than **5,000 employees** and annual revenue exceeding **EUR 1.5 billion**.

A key change is the **abolishment of the requirement to adopt a transformation plan for climate change mitigation**. The updated rules also remove the harmonized EU liability regime.

For the incorrect application of the rules, businesses will be held liable at the national level, with a new **maximum penalty** set at **3% of the company's global annual turnover**.

The deadline for Member States to transpose **CS3D** into national law is extended to **26 July 2028**, with companies required to comply with the new measures by **July 2029**.

Guidelines on the Regulation of Foreign Subsidies (FSR)

The **European Commission** has published **Guidelines on the application of certain provisions of the European Parliament and Council Regulation (EU) 2022/2560** on foreign subsidies distorting the internal market.

These guidelines clarify several key concepts:

- how the Commission assesses the distortion of competition caused by foreign subsidies,
- how negative effects are balanced with potential positive impacts, and
- how the Commission exercises its power to require

prior notification even in cases below the established thresholds.

In assessing the distortion of competition, the Commission first examines whether the foreign subsidies strengthen the competitive position of the company in the EU. For subsidies that do not primarily target economic activities within the EU, a more detailed analysis is conducted to assess the risk of their use for cross-subsidization. The Commission then considers the impact on competition by analyzing whether the subsidy is likely to change the competitive behavior of the company to the detriment of other economic entities.

A specific approach is applied in public procurement procedures, where the Commission first assesses whether the economic entity could have used the foreign subsidy in designing the terms of its offer. If this is the case, the next step is to evaluate whether the submitted offer is disproportionately advantageous compared to other offers and the contracting authority's estimates, and whether this advantage largely arises from the foreign subsidy or from other justified factors.

As part of the so-called **balancing test**, the Commission weighs the negative effects of the foreign subsidies against their specific positive effects. The severity of the distortion and whether the positive effects could have been achieved without the subsidy are also considered. If the positive effects outweigh the negative ones, the Commission will raise no objections. However, if the negative effects prevail, it may impose commitments or corrective measures.

The guidelines also clarify the **"call-in" mechanism**, which allows the Commission, under certain conditions, to request prior notification of otherwise non-notified mergers and acquisitions, and financial contributions in public procurement procedures. In all cases, however, the Commission must intervene before the mergers are fully implemented or the contracts are awarded.

A new feature is the introduction of "safe harbors", which exempt from this mechanism procurement procedures for low-value contracts, subsidies below EUR 4 million, and subsidies addressing certain exceptional circumstances.

Weinhold Legal

Digital Legal Update

SPRING 2026

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