Key **Life Sciences and Healthcare** developments and expectations for 2026

CEE and **Adria** region

2026

Table of **contents**

Hot topics

NIS2, data privacy, AI

Market access and reimbursement

Anti-corruption and compliance

Product liability

Countries

NIS2, Data Privacy, AI

Key developments to watch

NIS2 Directive transposition:

After the failure of NISG 2024, **Austria's NISG 2026 will transpose the EU NIS2 Directive into national law and significantly broaden the cybersecurity framework for "essential" and "important" entities**. It centres on risk-based security and governance obligations, stricter incident reporting requirements (including early initial notifications within short deadlines and follow-up reports), mandatory supply-chain security measures, and clearer management accountability with sanctions for non-compliance.

Compared with the current regime, more sectors and companies will be in scope based on size and criticality, and organisations will be required to implement systematic information security management systems, business continuity and crisis processes, as well as regular audits and technical measures such as patch and vulnerability management, access controls, and encryption.

EU-level changes driving Austrian practice

- **European Health Data Space (EHDS).** The forthcoming EHDS will introduce a harmonised framework for primary and secondary use of electronic health data, national health data access bodies, and participation in HealthData@EU infrastructure. Expect phased applicability over the next few years, with Austria needing to designate a health data access body and adapt its e-health infrastructure (e.g. ELGA).
- **EU Data Act.** Taking effect in stages through 2025 and 2026, the Data Act expands access rights to data from connected products and related services, along with cloud switching obligations.
- **AI and health data.** The EU AI Act will impose risk-based obligations for high-risk systems, including many clinical and medical device AI uses. Expect additional transparency, data governance, and post-market monitoring duties that intersect with GDPR principles (lawfulness, fairness, bias mitigation, data quality) for training and validation datasets.

Impact on the life sciences sector

NIS2 Directive transposition:

For the life sciences sector, including healthcare providers, pharmaceutical manufacturers, medical device companies, laboratories, biotech firms, and CROs, this will likely mean classification as essential or important entities, depending on activities and company size. In practice, priorities include establishing or adapting an ISO 27001-aligned ISMS, tightly integrated incident response and reporting processes (including alignment with data protection requirements), stricter supplier and cloud due diligence, securing production and laboratory OT, and hardening clinical trial infrastructures.

Boards and managing directors will face heightened duties to oversee the effectiveness of security measures, alongside increased audit and evidencing obligations and potentially significant fines. Overall, NISG 2026 raises the industry baseline in life sciences towards end-to-end resilience across research, development, manufacturing, and supply chains.

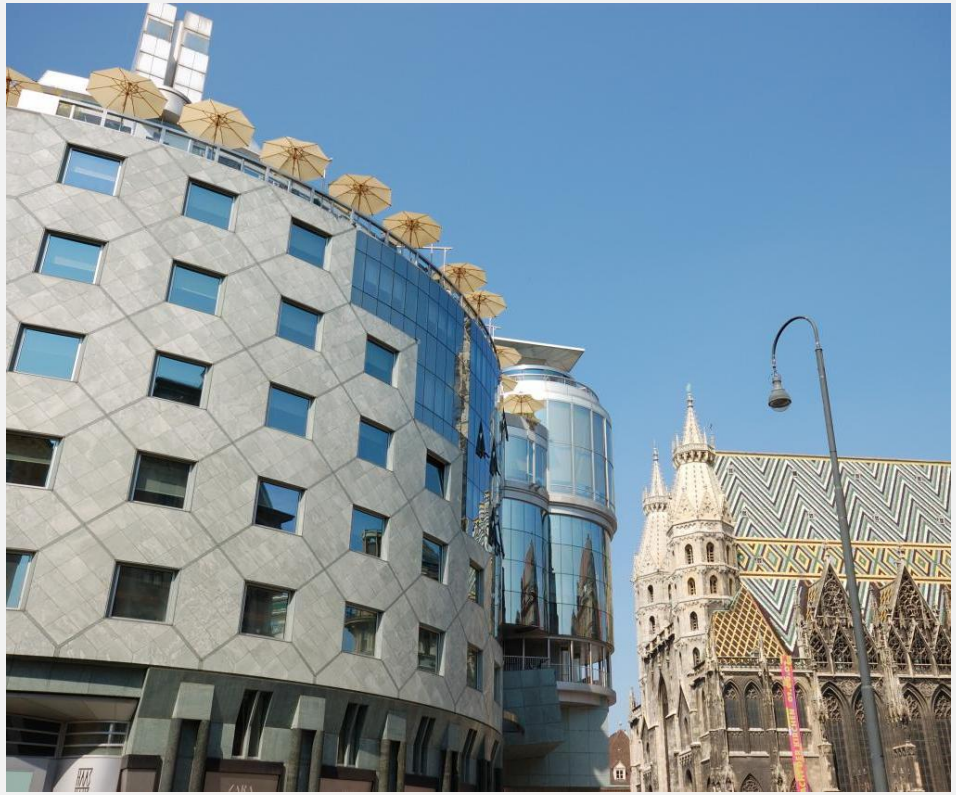
EU-level changes driving Austrian practice

- **European Health Data Space (EHDS).** Life sciences impacts include standardised procedures for secondary-use permits, stricter data minimisation, robust pseudonymisation/ anonymisation requirements, and tighter conditions for cross-border data access for research.
- **EU Data Act.** For life sciences and MedTech, watch for implications for access to and sharing of device-/sensor-generated data, interaction with trade secrets, and constraints on processing of personal and special-category data under the GDPR (which continue to prevail). The access rights granted by the Data Act in combination with the GDPR create a legal situation in which every mistake is punished. If non-personal data is unlawfully not shared, this constitutes a violation of the Data Act. If personal data is incorrectly classified as non-personal and shared, this constitutes a violation of the GDPR. Accordingly, every decision to share or not to share data must be carefully considered.
- **AI and health data.** AI systems processing health and medical data will most likely be subject to the AI Act's strictest requirements targeted at high-risk systems.

Product liability

Key developments to watch

- **Austria must implement the Product liability Directive by the end of 2026.**
- So far, **no proposal has been published.**
- The Austrian Supreme Court confirmed in recent case law that a manufacturer that is based outside the EEA cannot be sued for damages in Austria in the absence of any links to Austria. Failure to comply with product monitoring and vigilance obligations in Austria does not establish such a link.



Product liability

Key developments to watch

Introductory specifics on Bosnia and Herzegovina

Bosnia and Herzegovina ("BiH") has a complex constitutional and legislative composition. It consists of two entities: the Federation of Bosnia and Herzegovina ("FBiH") and Republika Srpska ("RS") and the Brčko District, a condominium. Furthermore, there are ten cantons in the Federation of Bosnia and Herzegovina.

This means that legislation is introduced at several levels and the topic of product liability in the Life Sciences sector is regulated by numerous and dispersed legislation, an overview of which is presented below.

Laws of general application relevant to product liability in Life Sciences

Laws on Obligations applicable in RS and FBiH (civil (tort) and contract law code): liability for damages envisaged as well as presumption of causation:

- Law on general product safety adopted at state, BiH, level: a general manufacturer's duty to only place safe products on the market envisaged;
- Law on market surveillance in BiH: various corrective measures can be issued by supervisory bodies, including a withdrawal or a recall order of a product; and
- Consumer protection laws introduced at both state (BiH) and entity (RS) levels contain various provisions on liability for products/goods and numerous contract and consumer protection remedies.

Specific regulations – medicines and medical devices

In BiH, an extensive regulatory framework is imposed under the Law on medicines and medical devices at the state, BiH, level which regulates liability for medicines and medical devices products of various market participants (including the manufacturers, marketing authorisation holders, importers, etc.):

- the regime places several regulatory obligations on such parties; and
- the Agency for Medicines and Medical Devices of BiH (ALMBiH) is the competent supervisory authority in this sector and holds extensive powers to issue a catalogue of supervisory measures, including product ban and/or recall, suspension of marketing licences and alike.

Impact on the life sciences sector

The "EU Outlook"

Bosnia and Herzegovina formally applied for EU membership in February 2016 and was granted EU candidate status in December 2022 by the European Council.

As a candidate country, **BiH is expected to gradually align its domestic legislation with the EU acquis**, both in terms of substantive content and enforcement.

This is visible through various pieces of existing or incoming pieces of legislation, and it can certainly be expected that significant regulatory developments will arise across the various areas of law in the near future, with an unavoidable impact on the life sciences sector.

NIS2, Data Privacy, AI

Key developments to watch

NIS2

In February 2026, Bulgaria adopted an amendment to the Bulgarian Cybersecurity Act (**the CA**) to transpose Directive (EU) 2022/2555 (**NIS2**). In line with NIS2, Annex I "**Sectors of high criticality**", Annex I of the CA covers healthcare providers, EU reference laboratories, entities carrying out research and development activities of medicinal products, entities manufacturing basic pharmaceutical products and pharmaceutical preparations, and entities manufacturing medical devices considered critical during a public health emergency (public health emergency critical devices list).

Size thresholds

Entities fall within the scope of the CA if they qualify as medium-sized enterprises under the Small and Medium-Sized Enterprises Act (the **SME Act**) or exceed that threshold and provide services or activities in the EU ('essential entities'), and entities that fall within the NIS2 exceptions to the size thresholds, including for instance where the entity distributes a service with significant impact on public safety, public security or public health.

Risk management measures

Essential entities must adopt appropriate and proportionate technical, operational, and organisational measures to manage risks to the security of network and information systems used in their core activities and service provision. Measures must be technology-neutral, account for the latest developments and relevant European and international standards, and ensure security in line with the identified risks. The required measures should cover policies and practices relating to risk management and risk assessment, incident response, business continuity, supply chain and system security, cyber hygiene and staff training, and the use of encryption, among others.

Management body accountability

The management bodies of essential entities must approve and oversee the implementation of cybersecurity risk-management measures. The members of management bodies are required to undergo cybersecurity training every two years and to organise regular training for their employees.

Incident reporting obligations

Essential and important entities must notify the sectoral Computer Security Incident Response Team (CSIRT) of any significant incident according to the following timeline:

- **Within 24 hours** of becoming aware of a significant incident: early warning indicating whether the incident is suspected to be caused by unlawful or malicious acts and whether it could have a cross-border impact.
- **Within 72 hours** of becoming aware of the incident: an incident notification must be submitted updating the early warning and providing an initial assessment of the incident, including its severity and impact, as well as any available technical information.
- **Within one month of the incident notification,** an interim report (if the incident is not yet resolved) or a final report must be submitted, containing a detailed description of the significant incident, its severity and impact, a root cause analysis, any cross-border impact, and the remediation measures applied. In any case, the final report must be submitted within one month of the incident's resolution.

Control and sanctions

Control over compliance is exercised by state bodies, including the national competent authority for the sector, **which must be designated by the Council of Ministers by August 2026**.
For essential entities, the authorities may temporarily suspend licences, registrations, certificates, or authorisations, or where such permits are not issued by the same authority, seek a court order or address the relevant competent authority to impose the interim measure.

Non-compliance may result in significant fines for the organisation and its management. Essential entities **may be sanctioned up to EUR 10 million or 2% of their global annual turnover**. Members of the management body may be held personally liable and fined up to EUR 5,000 for breaches of their obligations under the CA.

If the breach involves personal data, the Commission for Personal Data Protection may impose a sanction under data protection law. In such cases, if the data protection authority has already imposed a financial penalty for the same infringement, the cybersecurity authority should not impose an additional fine for that same violation.

Market access and reimbursement

Key developments to watch

NHIF Reimbursement Mechanism According to SAC Rulings

The Bulgarian Health Insurance Act requires a mechanism to ensure the predictability and sustainability of the National Health Insurance Fund (**NHIF**) budget for medicinal products included in the Positive Drug List (**PDL**). In practice, this mechanism shifts the burden of underfunding to marketing authorisation holders (**MAHs**). In April 2024, the Supreme Administrative Court upheld a ruling abolishing the 2021 Mechanism, finding it violated Article 19 of the Constitution of the Republic of Bulgaria, which guarantees freedom to conduct a business and uniform legal conditions for economic activity. The court determined that MAHs were obliged to cover 100% or more of the NHIF's excess expenses, effectively eliminating any profit from their commercial activities. MAHs of medicinal products with new INNs face a particularly serious burden, as the entire expenditure for such products is considered excessive, requiring compensation of more than 100% of NHIF expenditure. The Supreme Administrative Court found that the NHIF budget, while appearing balanced, actually conceals a deficit transferred to private entities/MAHs. Subsequent mechanisms adopted by the NHIF have largely reproduced the same irregularities. The currently applicable 2025 Mechanism has again been appealed before the Supreme Administrative Court.

Product liability

Key developments to watch

Bulgaria must implement the Product liability **Directive (EU) 2024/2853** by the **end of 2026**. So far, no proposal has been published.

NIS2, Data Privacy, AI

Key developments to watch

Cybersecurity

Regulation (EU) 2022/2555 ("NIS2") has been transposed into Croatian law through the Cybersecurity Act and Cybersecurity Regulation, foreseeing certain obligations for the essential and important entities, including those in the healthcare sector. **The Cybersecurity Act ("CA")** serves as a general transposition act regulating procedures and measures for achieving a high common level of cybersecurity, criteria for categorising key and important entities, cybersecurity requirements for key and important entities, etc. On the other hand, the **Cybersecurity Regulation ("CR")** serves as an implementing regulation, providing more detail approach to cybersecurity measures and obligations of both the competent authorities and the key and important entities subject to the CA.

While legislature was passed and came into force in 2024, 2025 was an important year for more detailed transposition. In February 2025, **the National Centre for Cybersecurity ("NCSC")** was established within **the Security Intelligence Agency ("SOA")**, with the aim of protecting national cyberspace and performing the tasks of the central state body for cybersecurity, the competent body for the implementation of cybersecurity requirements, the CSIRT, the body responsible for cyber crisis management, and the single point of contact under the Cybersecurity Act. The NCSC has since then passed several subordinate standards, methods and guidelines, providing more detailed instructions for subjects of the CA and CR.

In Q1 2025, the competent authorities for the implementation of cybersecurity requirements (including the NCSC) started conducting a coordinated process of categorising entities subject to the CA. From the NCSC report at the end of 2025, it is evident that 780 legal entities (159 key and 621 important entities) subject to the CA have been categorised in Croatia and have begun the coordinated implementation of cybersecurity measures and reporting cyber incidents.

AI

The Croatian legislator is in Q1 expected to pass an act implementing Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (EU).

European Health Data Space

The act on the implementation of Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Area (EU) is supposed to be passed in Q1 2026.

CONTINUED

NIS2, Data Privacy, AI (continued)

Impact on the life sciences sector

Cybersecurity and healthcare sector

As is the case with the NIS2 Directive, Annex I of the CA **"Sectors of high criticality"** lists healthcare providers, EU reference laboratories, entities carrying out research and development activities of medicinal products, entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2, and entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list). In addition to the NIS2, **the CA defines terms:** (a) healthcare provider as any individual person or legal entity that performs healthcare activities in the Republic of Croatia in accordance with the law regulating healthcare, excluding organisational units of the Ministry of Defence and Armed Forces of the Republic of Croatia and the ministry responsible for justice that perform healthcare activities under special regulations; (b) medicinal product as any substance or combination of substances shown to have properties for treating or preventing disease in humans or any substance or combination of substances that can be used or applied to humans for the purpose of restoring, correcting or adjusting physiological functions by pharmacological, immunological or metabolic action or for making a medical diagnosis.

As the NIS2, **Annex II** of the CA, **"Other critical sectors"**, lists manufacturers of medical devices and in vitro diagnostic medical devices, as defined in the applicable Regulation 2017/745 on medicinal devices and Regulation 2017/746 on in vitro diagnostic medicinal devices, except subjects – producers of medicinal devices – which are already mentioned Annex I.

Whether they constitute key or important entities depends on their size. While important entities are those that constitute medium-sized small business, key entities are those which exceed the upper limits for medium-sized small businesses as defined under the Croatian Act on Encouraging the Development of Small Businesses. Additionally, healthcare entities listed in Annex I or II may be designated as key or important, regardless of their size, if they are the only essential service provider, if a disruption could significantly affect public safety, protection or health, if it could cause systemic risks (including cross-border), or if the entity is particularly important at a national, regional or local level.

Deviating from the NIS2 Directive, **the Croatian Cybersecurity Act applies to those entities that are registered in Croatia and carry out activities in the EU**. There are additional exceptions regarding entities from digital infrastructure and digital services sector.

Regarding the registration process, although the mandatory content for reporting in NIS2 and CA is the same, the procedure is different. The CA provides that, instead of registering and providing the regulatory body with this information, entities (e.g. a private clinic) must submit the relevant information at the regulatory body's request. The CR prescribes detailed obligations regarding: (i) the designation of a contact person; and (ii) the notification procedure of data relevant for registration and for the appointment of the designated contact person.

The CA and CR do not deviate much from the NIS2 regarding cybersecurity measures which key and important entities are obliged to conduct. Therefore, healthcare entities subject to the cybersecurity regime are obliged to report significant incidents and serious cyber threats, as well as conduct cybersecurity risk-management measures. The Cybersecurity Regulation further specifies cybersecurity risk management measures in its Annex II "Cyber security risk management measures" and **Annex III "Special physical security measures for entities in the digital infrastructure sector"**.

Market access and reimbursement

Key developments to watch

Changes to Croatian Medicines Act ("MA") created a new regime for ensuring continuous supply of medicinal products to the Croatian market. While Croatian Agency for **Medicinal Products and Medical Devices ("HALMED")** remains responsible for monitoring the supply of medicinal products to the territory of Croatia, now also the Ministry of Health ("Ministry") is responsible to conduct activities necessary to ensure continuous supply of medicinal products to Crotian market.

In the new regime, Marketing authorization holders (**"MAH"**), distributors, wholesalers and importers are, within the scope of their responsibilities, obliged to notify HALMED, Ministry and sometimes Croatian Institute for Health Insurance (**"HZZO"**) in writing and without delay of any circumstances that may lead to disruption of the supply of medicinal products to the Croatian market or a shortage of medicinal products or/and on planned quantities of medicinal products and stocks of medicinal products for the Croatian market.

Such notification must be done in electronic form via the special information system for monitoring and preventing shortages of medicinal products in the Republic of Croatia.

Impact on the life sciences sector

The new changes have an impact on the life science sector since the new legislative change ensured more explicit obligation for MAH, distributors, wholesalers and importers to notify relevant authorities of any circumstance. **Specifically:**

a) **Marketing authorisation holders** (**"MAH"**) must:
   - notify HALMED and the Ministry of Health (**"Ministry"**) in writing without delay of any circumstances that may lead to a disruption in the supply of medicinal products to the Croatian market or a shortage of medicinal products, and also notify the Croatian Institute for Health Insurance (**"HZZO"**) for medicinal products included on the list of medicinal products of HZZO;
   - regularly provide HALMED and the Ministry with data on the planned quantities of medicinal products and stocks of medicinal products for the Croatian market, in electronic form via the information system.

b) **Whole traders** (i.e. legal entities and individual persons who carry out wholesale trade in medicinal products in accordance with the Medicines Act and who carry out parallel trade and parallel import of medicinal products in the Republic of Croatia) must regularly submit data to the HALMED and the Ministry on planned, ordered and delivered quantities of medicinal products and stocks of medicinal products for the Croatian market, in electronic form via the information system.

c) **Other traders** (i.e. legal entities and individual persons engaged in retail trade in medicines in accordance with Medicines Act in the Republic of Croatia) must regularly submit data to HALMED and the Ministry on planned, ordered and dispensed quantities of medicines and stocks of medicines for the Croatian market, in electronic form via the information system.

d) **Wholesalers and importers** are obliged, regarding the extraordinary entry or import of medicines which do not have marketing authorisation but have HALMED's consent due to:
   - a medically justified need or the protection of human health;
   - natural disasters or other emergencies;
   - necessary cases of individual treatment with a medicinal product prescribed on its own responsibility by a medical doctor or a dentist who is providing the treatment;

   to regularly submit data to HALMED and the Ministry on ordered and delivered quantities of medicines for the Croatian market, in electronic form via the information system.

NIS2, Data Privacy, AI

Key developments to watch

Cybersecurity

The new Act No. 265/2025 Coll., ("Czech Cybersecurity Act") came into force on 1 November 2025. The Czech Cybersecurity Act imposes new obligation on hospitals, laboratories, medical devices, digital health services, telemedicine.

AI

Regulation (EU) 2024/1689, Artificial Intelligence Act (the "EU AI ACT") directly applies in the Czech Republic. The EU AI ACT establishes harmonised rules for AI, which sets specific requirements for AI systems based on their risk levels to safety, health, and fundamental rights, came into force on 1 August 2024. The rules set down in the EU AI ACT take effect gradually.

The Czech government is preparing a national Act on Artificial Intelligence to complement the EU AI Act, which is expected to be adopted in 2026 (the **"Czech Implementing Act"**).

Data Privacy

New European Health Data Space Regulation ("EHDS") came into force in March 2025. It aims to enable the secure sharing of health data across the European Union

Impact on the life sciences sector

Cybersecurity

NIS2: Czech Act No. 265/2025 Coll., the Cybersecurity Act imposes security obligations on operators of critical information systems and digital service providers, such as implementing mandatory technical and organisational measures such as regular penetration tests, cyber threat monitoring, mandatory incident reporting and others. As of 1 November 2025, organisations have 60 days to self-identify and report regulated services to the National Cyber and Information Security Agency.

AI

The EU AI Act uses a risk-based classification, grouping AI systems into four risk-categories, ranging from unacceptable to minimal risk.

Medical and health technologies: AI in medical devices and robot-assisted surgery is treated as high-risk; data protection rules, medical device rules, and product safety/liability also apply. The EU AI Act adds a layer of regulatory requirements for medical device firms already governed by the Medical Device Regulation (MDR 2017/745).

Data Privacy

The EHDS should frame easier access to secondary-use health data for research, including clinical studies. It imposes new obligations on data holders (hospitals) and data users (pharmaceutical companies). Hospitals need new IT infrastructure, must transform unstructured notes into shareable datasets, and change health data into compatible format easy to share.

Market access and reimbursement

Key developments to watch

Although there are no material changes to market access and reimbursement concerning pharmaceuticals and medical devices, there are partial changes and ongoing discussions. In addition, a new Czech government has recently been elected and it is likely that the Ministry of Health may proceed with further and more significant changes.

Impact on the life sciences sector

There are partial changes concerning the reimbursement of highly innovative pharmaceuticals and ongoing discussions concerning the potential deregulation of pricing of certain types of medical devices. The legislative process should continue to be monitored.

Anti-corruption and compliance

Key developments to watch

There are no material changes to anti-corruption and compliance specifically for the Czech Republic. On the EU level, the Parliament and Council reached a provisional agreement on the EU's first-ever directive harmonising criminal laws to fight corruption, strengthening efforts to prevent, prosecute and punish offences across the EU (Agreement reached on the first EU-wide criminal law rules against corruption | Aktuelles | Europäisches Parlament).

Impact on the life sciences sector

The Czech Republic's anti-corruption and compliance framework remains unchanged, with no significant current or forthcoming reforms specific to pharmaceuticals or medical devices.

Product liability

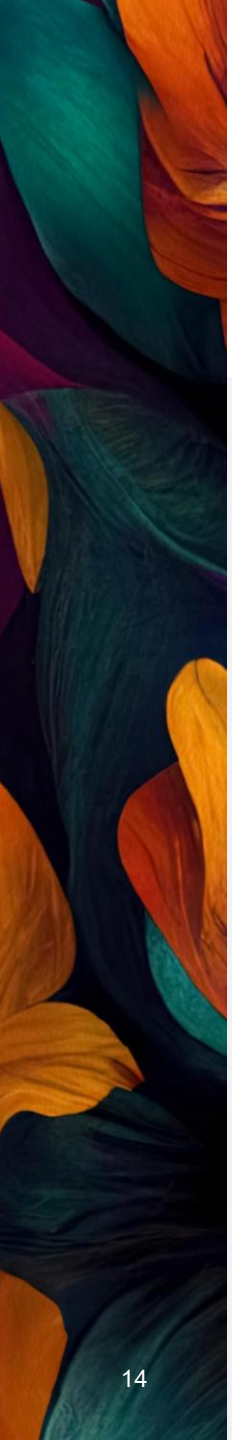
Key developments to watch

The Ministry of Industry and Trade is currently preparing to transpose the EU Product Liability Directive into Czech law.

Transposition needs to be completed by 9 December 2026, and the Ministry aims to finalise the draft legislation by 31 March 2026 to allow sufficient time for the subsequent legislative process.

Impact on the life sciences sector

The new rules will significantly impact the whole life sciences sector and various members of the supply chain, including manufacturers, importers and distributors. The legislative process should continue to be monitored.



Product liability

Key developments to watch

NIS2

Hungary amended Act LXIX of 2024 on the cybersecurity of Hungary which implements NIS2 (and complies with the CRA). The amendment was published in the Official Gazette on 29 December 2025.

A new provision will ensure that entities listed in Annexes 2-3 of the Cybersecurity Act will fall within the scope of the legislation if either of the following thresholds is met:

- the total number of employees is 50 or more; or
- annual net turnover exceeds EUR 10 million, and the total balance sheet exceeds EUR 10 million.

The legislation introduces a new ground for refusal of data access requests.

GDPR and data privacy

- The European Commission published its "Digital Omnibus" proposal on 19 November 2025, a major horizontal legislative proposal that both consolidates parts of the EU data acquis into the Data Act and introduces targeted GDPR amendments. It repeals the Free Flow of Non-Personal Data Regulation, the Open Data Directive, and the Data Governance Act, while transplanting key provisions into the Data Act to create a single, streamlined legal instrument for Europe's data economy.
- The package also establishes a single notification portal (developed by ENISA) to centralise incident- and event-reporting under the GDPR, DORA, NIS2, eIDAS, and CER.
- Trade secret holders gain a new ground to refuse data-access requests where there is a high risk of unlawful acquisition, use, or disclosure to third countries (including SOEs) with weaker protections.

Artificial Intelligence

Hungarian statutory developments on AI: Hungary has established a national enforcement framework for the EU AI Act via Act LXXV of 2025 and Government Decree 344/2025, with a broad jurisdiction that captures any use of AI system outputs in Hungary, regardless of where the system was marketed or the provider is established.

Impact on the life sciences sector

NIS2

Mid-sized pharmaceutical companies, biotech firms, CROs, clinical trial service providers, med-tech manufacturers and digital health companies, many of which were previously outside or doubtfully within scope, will now be unambiguously regulated. This reduces legal ambiguity but significantly increases compliance obligations (registration, audits, incident reporting) for R&D-heavy but non-critical-infrastructure actors. In practice, Hungary becomes a stricter jurisdiction than the NIS2 minimum for life sciences companies operating at scale but not traditionally viewed as "critical".

GDPR and data privacy

For companies in the life sciences sector, the single reporting point under the GDPR, DORA, NIS2, eIDAS and CER means a significant simplification regarding their incident reporting obligations.

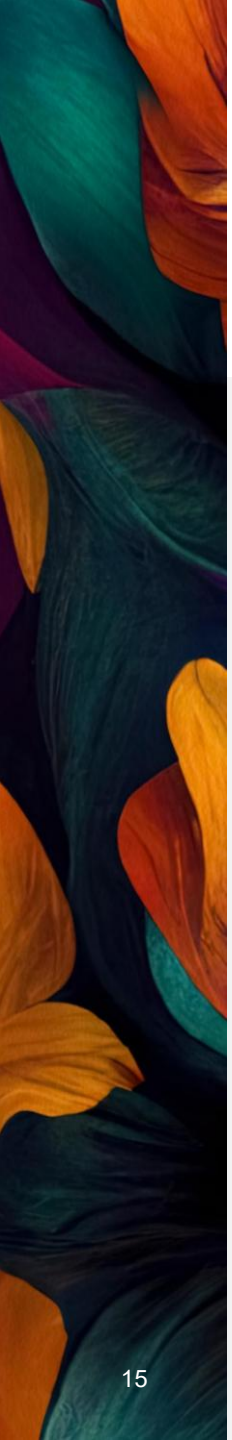
NIS2 implementing Act LXIX of 2024 on the cybersecurity of Hungary ensures a new ground of refusal to disclose certain types of data.

Furthermore, the tightening of B2G data access to true public emergencies and the strengthened trade-secret and third-country safeguards are particularly valuable for protecting clinical data, manufacturing know-how and AI training assets from over-broad disclosure risks.

Overall, the Commission expects EUR 5 billion in cost savings for businesses across the EU by 2029.

Artificial Intelligence

Life sciences manufacturers and deployers using AI in medical devices, diagnostics, clinical decision support, or hospital workflows should align MDR/IVDR technical files and post-market surveillance with AI Act obligations on risk management, data quality, bias, robustness, transparency, and human oversight, anticipating market surveillance reviews.



Anti-corruption and compliance

Key developments to watch

Hungary is undertaking a significant reform of its corporate criminal liability regime following amendments to the Corporate Criminal Code adopted on 11 June 2025:

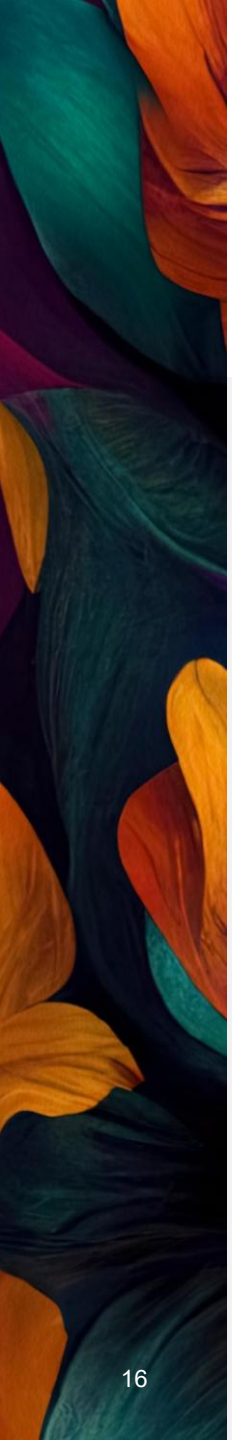
- The reform responds to the rapid evolution of corporate criminal law and seeks to balance effective enforcement with safeguards against disproportionate sanctions.
- Its overarching goals include clarifying existing rules, increasing flexibility in applying measures to legal entities, and fostering cooperation between corporations and law-enforcement during investigations.
- The amendment also emphasises prevention by encouraging stronger internal control systems and proportionate sanctioning frameworks.
- A key change is the extension of the code's scope so that, from 2026, foreign corporations may be held criminally liable if their offence falls under Hungarian criminal jurisdiction.
- This expanded jurisdiction aligns Hungary with directive (EU) 2024/1226, reflecting broader EU efforts to combat cross-border crime effectively.
- Liability is also extended to legal successors and newly formed organisations that assume the economic or organisational structures derived from an offence.
- The previous requirement that corporate measures apply only where an intentional offence occurred has been removed, allowing sanctions even when offences were committed negligently.
- Corporate liability may now arise where an executive negligently fails to recognise and prevent criminal acts committed by employees or members.
- Corruption offences receive particular attention under the new framework, increasing companies' exposure when employee misconduct results in unlawful financial advantage.

Impact on the life sciences sector

Strengthened **corporate criminal liability rules in Hungary** mean that pharmaceutical companies face higher exposure to sanctions even for negligent offences, including situations where company resources are used or where executives fail to prevent employee misconduct.

This is particularly relevant given **the compliance-sensitive nature of pharma operations**, where interactions with healthcare professionals, public health bodies, and reimbursement authorities already pose heightened regulatory and corruption-related risks.

Additionally, with **liability extending to foreign entities and legal successors, multinational pharma groups operating in Hungary** may need to tighten internal controls, auditing systems, and documentation practices across affiliates to manage cross-border compliance risks an area already prominent in pharma compliance investigations in the region.



Product liability

Key developments to watch

The Civil Code's product liability rules were recently modified by Act XCII. Of 2025 on the amendment of private law statues to comply with the new revised Product Liability Directive (PLD).

The main changes are:

- Section 21. § (3) of the Act XCV. of 2005 on Medicinal Products for Human Use and on the Amendment of Other Acts Regulating the Pharmaceutical Market is amended to apply the new product liability regime of the Civil Code.
- Sections 6:550–6:559 of the Civil Code are rewritten in their entirety to align with the new Product Liability Directive (Directive (EU) 2024/2853).
- Applicable after 9 December 2026.
- Expansion of the definition of "product"
- Changes to the definition of "product damage"
- New factors for assessing product defectiveness, including aspects specific to AI systems: "In assessing whether a product is defective, particular regard must be given to: […]
  - any effect on the product of its capacity for continuous learning or for acquiring new features after being placed on the market or put into service; […]
  - the applicable product-safety requirements, including cybersecurity requirements relevant to safety; […]."
- The rules on exemptions from product liability also change.

Introduction of a rebuttable presumption of defect.

Impact on the life sciences sector

The amendment materially raises liability exposure for life sciences manufacturers by expanding **"product" to cover software, digital files, and connected components, bringing SaMD, AI-enabled diagnostics, and hospital IT integrations squarely within the product liability net.**

It aligns defect analysis with AI- and cyber-specific factors (continuous learning, interoperability effects, and cybersecurity requirements), which will pressure PMS/vigilance systems to evidence safe updates, change control, and real-world performance across device lifecycles.

The tightened exemptions, especially where defects relate to associated services, software or missing safety updates under the manufacturer's control, reduce room to shift blame to vendors, making update cadence and secure-by-design engineering legally pivotal.

The new rebuttable presumptions of defect (e.g., for obvious malfunctions or unmet safety requirements, or where material evidence isn't disclosed) lower evidentiary hurdles for claimants, elevating litigation and insurance stakes.

NIS2, Data Privacy, AI

Key developments to watch

- North Macedonia adopted a **new Law on the Security of Network and Information Systems in July 2025 (“Cybersecurity Law”)**, to align with the EU NIS2 Directive. The Cybersecurity Law came into force 1 January 2026.
- The Cybersecurity Law applies to **medium and large entities providing services in the healthcare sector, as well as in manufacturing**, where it explicitly includes companies engaged in the production of medical devices and in-vitro diagnostic medical devices. In addition, the law also applies to companies whose services have a significant impact on public health.
- The general obligations applicable **to all in-scope entities include the appointment of a representative in North Macedonia where no local registered seat exists**, and the submission of annual reports to the Ministry of Digital Transformation. Additional statutory obligations apply specifically to entities classified as “essential” or “important”, depending on their size and type of activity.

Impact on the life sciences sector

The general obligations arising from the Cybersecurity Law for entities are to:

- adopt an annual cyber risk assessment, approved and overseen by management, and provide regular cybersecurity training to employees;
- implement security measures covering incident response, business continuity/disaster recovery, supply chain security, secure development and vulnerability handling, effectiveness testing and cyber hygiene, strong access controls and multi factor/continuous authentication, and secure communications;
- assess and manage supplier/ICT security; use of certified ICT may be required; and high-risk noncompliant ICT may be excluded from public procurement;
- appoint a cybersecurity officer (for essential entities) to liaise with the authority and national cybersecurity incident response teams (CSIRT);
- notify significant incidents to the CSIRT immediately and within three hours, followed by a 24-hour early warning, a 72-hour incident report, and a final report within one month; inform affected users by the next working day where relevant;
- undergo supervision and, where required, audits; and comply with binding instructions and corrective measures.

Administrative fines for non-compliance can be up to 2% of the previous year’s global turnover for essential entities and up to 1.4% for important entities, alongside potential personal fines for the responsible persons.

NIS2, Data Privacy, AI

Key developments to watch

Poland completed the transposition of the NIS2 Directive on 19 February 2026, when the amendment to the Act on the National Cybersecurity System implementing the Directive was signed by the President.

Notably, the Polish Act expands the list of essential and important entities in the life sciences sector, going beyond the minimum regulatory expectations set by the Directive.

The Act is scheduled to enter into force on 3 April 2026, notwithstanding the President's referral to the Constitutional Tribunal for an ex-post review – raising concerns, among others, over the Act's expansion to economic sectors beyond EU requirements and disproportionately severe administrative penalties – which does not suspend the legislation's validity unless the Tribunal declares it unconstitutional.

Draft of the Polish Act on AI systems: Poland is still working on a national law to complement the EU AI Act, known as the Draft Act on AI Systems. The latest version was published on 24 February 2026, but it has not yet reached the parliamentary stage.

The proposal aims to align local regulations with the EU framework by establishing national supervisory authorities, defining compliance and enforcement procedures, introducing administrative fines, and supporting AI development through measures such as regulatory sandboxes and funding for SMEs.

Impact on the life sciences sector

The broadening of the scope under the **Polish Act on the National Cybersecurity System** means that more life sciences organisations, compared to those captured by the NIS2 Directive alone, may be classified as essential or important entities. Such classification will trigger extensive cybersecurity and reporting obligations, making early preparation critical.

The sector should therefore proactively assess its potential status under the new law and begin strengthening internal cybersecurity frameworks, especially given that the transition period following adoption is expected to be short.

In parallel, **the Draft Act on AI Systems will operationalise the EU AI Act in Poland** by establishing national authorities, procedures and fines, and enabling tools such as regulatory sandboxes and SME support. For life sciences that develop, deploy or procure AI in R&D, clinical, diagnostics or manufacturing, this will introduce stricter governance, documentation and incident-reporting expectations.

Companies should monitor these developments, as active monitoring and early preparation will minimise compliance and operational risk.

Market access and reimbursement

Key developments to watch

Poland is progressing with another major amendment to the reimbursement law (the "SZNUR"), intended to refine and soften several regulatory burdens introduced by the **2023 Big Reimbursement Amendment (the "DNUR").**

The new package aims to simplify administrative requirements, shorten reimbursement timelines, and introduce more flexible mechanisms such as special rules for orphan drugs and a new reimbursement category covering therapies used across both outpatient and hospital care. **Parallel work on aligning national processes with the EU's joint HTA framework is expected to streamline evidence requirements and increase predictability for manufacturers.**

Impact on the life sciences sector

Together, these initiatives represent a major overhaul of Poland's market access and reimbursement landscape. For the life sciences sector, the reforms may shorten time-to-market, enhance the predictability of reimbursement procedures, and create new strategic opportunities in pricing negotiations and launch planning.

However, it **remains essential to closely track further legislative updates, as key requirements for reimbursement and reporting may still evolve.**

Anti-corruption and compliance

Key developments to watch

In 2026, Poland may see a **new anti-corruption and compliance regime enter into force arising from a draft law currently going through the legislative process (with the first reading in the Parliament in late November)**, which would reorganise the institutional framework by dissolving the Central Anti-Corruption Bureau and reallocating its tasks to the Police and the National Revenue Administration, strengthen inter-agency cooperation, and expand preventive oversight of high-risk public projects.

On the EU level, a **new Anti-Corruption Directive is expected to be formally adopted in 2026 following the provisional deal reached in December 2025**, introducing harmonised definitions of corruption offences, minimum sanction levels and an obligation for each Member State to publish a national anti-corruption strategy, which will require subsequent adjustments to Poland's criminal and compliance framework.

Impact on the life sciences sector

For life-sciences companies that depend heavily on public procurement and interactions with hospitals and healthcare professionals, a draft Polish law reorganising anti-corruption enforcement **signals a shift this year towards more coordinated criminal and administrative scrutiny of tenders, sponsorships, reimbursement and grants**.

Considering the planned EU-level changes (introducing harmonised definitions of corruption offences, minimum sanction levels, and an obligation on each Member State to publish a national anti-corruption strategy) companies in **the sector should closely monitor the legislative process, as these standards will prompt subsequent adjustments in Poland's criminal and compliance framework.**

Product liability

Key developments to watch

Poland must transpose the new **EU Product Liability Directive 2024/2853 (PLD) by 9 December 2026**, which will operate alongside the already applicable General Product Safety Regulation (GPSR) and a forthcoming new Polish General Product Safety Act, together reshaping the liability and market surveillance landscape for producers, importers, distributors, and online marketplaces.

Importantly, the **new Polish General Product Safety Act has progressed to the final stage of the national legislative process**. In late November 2025, the Act was sent to the President for signature, which is the last step before promulgation. Once enacted, the Act will strengthen the Polish Competition and Consumer Protection Authority's (UOKiK) enforcement powers and allow fines of up to PLN 1 million for placing unsafe products on the market, including via e-commerce channels.

According to information published in a parliamentary interpellation in late November 2025, the **Civil Law Codification Commission is working on a draft to also implement the PLD into the Polish legal order**, with a preliminary plan indicating that the draft will be presented within the next six months.

Impact on the life sciences sector

For life-sciences companies, this means that not only medicinal products, medical devices and IVDs, but also **connected software, SaMD and AI-driven diagnostic or decision-support tools, may trigger strict product-liability exposure under the revised regime.**

The combined effect of the new PLD rules, stronger GPSR-based market-surveillance and recall powers and **Poland's updated collective-redress framework**, is likely to increase the volume and value of product-related claims, so businesses should already be mapping their portfolios against the new definitions and preparing to update risk assessments, vigilance systems, contractual allocations of risk and insurance limits.

NIS2, Data Privacy, AI

Key developments to watch

NIS2

Romania began implementing the NIS2 legislation, requiring entities to register with the Romanian Cybersecurity Authority (the **"DNSC"**) in 2025 and comply with a set of cybersecurity obligations within defined timeline. The DNSC is still developing enactments for the implementation of these obligations, which should be monitored.

AI

Romania will have to transpose the new Product Liability Directive, which will have an impact on AI liability.

Impact on the life sciences sector

NIS2

Actors in the life sciences sector can fall within the scope of the NIS2 legal framework. Romania especially deviated from the NIS2 Directive, adding to the list of relevant sectors.

AI

The rules should clarify who is liable for damage caused by AI systems. This should be relevant to life sciences entities that use AI for diagnostics, medical devices, drug discovery, and personalised medicine.

Market access and reimbursement

Key developments to watch

Law 163/2025 introduced certain amendments to the health-care system.

The law introduces a controlled-access mechanism for medicines not included in the reimbursed medicine list. Access to these medicines will be based on cost-sharing agreements between the NHIH and MAHs.

In addition, the law introduces a temporary solidarity contribution payable by MAHs, supplementing the existing quarterly claw-back contribution regime.

Impact on the life sciences sector

MAHs are directly affected by these changes.

Product liability

Key developments to watch

AI: Romania will have to transpose the new Product Liability Directive. So far, no draft law has been published. This situation should be monitored.

Impact on the life sciences sector

Impact on the liability of manufacturers and providers under the law.

NIS2, Data Privacy, AI

Key developments to watch

Serbia has taken a significant step towards strengthening cyber resilience with the introduction of a new Information Security Law (the “Law”) in October 2025. The by-laws envisaged under this Law should be adopted within 12 months from the date of its entry into force. Although Serbia is not an EU member, the Law aims to align with the principles and core mechanisms of the NIS2, Serbia has taken a significant step towards strengthening cyber resilience with the introduction of a new Information Security Law (the “Law”) in October 2025. The by-laws envisaged under this Law should be adopted within 12 months from the date of its entry into force. Although Serbia is not an EU member, the Law aims to align with the principles and core mechanisms of the NIS2, enhancing a safer and more reliable use of information and communication technologies (ICT).

Like the previous law, the new Law also applies to entities operating in critical sectors such as healthcare, but unlike the old law which applied only to the domain of healthcare provision, it now widens its scope to include:

- The operation of national reference laboratories.
- Research and development of medicinal products.
- The manufacturing of pharmaceutical medicines and preparations intended for healthcare use.
- The manufacturing of medicines and other products intended for use in healthcare, including products of vital importance during public health emergencies.
- The processing of genetic, biomedical data and other data relevant to research and development in the fields of biotechnology, bioinformatics, bioeconomy, genetics, and medicine.

A category of important ICT system operators is introduced, encompassing legal entities and natural persons in the capacity of registered subjects, engaged in activities related to the manufacturing of medical devices and the production of in vitro diagnostic medical products.

Regarding AI regulation, in January 2025 Serbia adopted the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for 2025–2030. This strategy lays the foundation for the further development of the legal and institutional framework, enabling the creation of solutions to numerous ethical and regulatory challenges. Above all, it serves as the basis for the future Law on Artificial Intelligence. It is expected that for high-risk systems, such as those in the healthcare sector, strict obligations will be introduced, similar to those established in the European Union.

Impact on the life sciences sector

The new Law has a significant impact on the healthcare sector as it encompasses a broader range of entities and activities in healthcare. As a result, healthcare institutions, pharmaceutical companies, and other relevant actors engaged in certain activities are classified as operators of ICT systems of special importance or operators of important ICT systems, which means they are required to implement strict cybersecurity measures and align with European standards such as NIS2. The practical effect is the strengthening of resilience across the entire healthcare ecosystem against cyber threats, improved protection of patient data, and a more secure continuity of healthcare services.

Among the key obligations introduced are the mandatory implementation of risk assessments and the adoption of a risk assessment act (to be revised at least annually), as well as a security assessment act. Entities are now required to report not only incidents, as was previously the case, but also serious threats to ICT systems of special importance. For operators of priority ICT systems of special importance, the frequency of compliance checks for ICT security measures has been increased to twice a year.

NIS2, Data Privacy, AI

Key developments to watch

Slovak implementation of NIS2 and the resulting obligations for the healthcare industry

The NIS2 Directive (EU) 2022/2555 replaces the earlier NIS1 framework and represents the EU's most substantial upgrade of cybersecurity rules to date. It strengthens requirements across essential sectors, including healthcare, with the aim of improving resilience against cyber threats.

Legislative background and implementation

Slovakia transposed NIS2 through Act No. 366/2024, which amends the Cybersecurity Act No. 69/2018 Coll. and hcompetentas been effective since 1 January 2025. The National Security Office (NBÚ), together with ministries, acts as the supervisory authority responsible for oversight, guidance, training, and maintaining the national registry of regulated entities.

A major change introduced by the new legislation is the shift in identifying obliged entities. Under NIS2, the previous two-part identification mechanism is replaced with a clear and exhaustive list of essential entities. The sectoral annex confirms that healthcare providers are explicitly listed as operators of critical essential services.

Key obligations for healthcare entities

- Self-assessment: whether they fall within the scope of the act. if they do, they must notify the NBÚ within 60 days of commencing a regulated activity.
- Essential healthcare entities must register in the NBÚ's jiskb portal.
- After registration in the national system, they must implement "required security" measures within 12 months and complete a mandatory audit or self-assessment within 24 months.
- Mandatory incident reporting: significant threats, near-miss events, vulnerabilities, and the handling of cybersecurity incidents, voluntary reporting.
- "Rapid" reporting: initial incident notification within 24 hours, detailed report within 72 hours, and a final report within 30 days.

Sanctions

The NBÚ may conduct ongoing supervision and inspections. Non-compliance may result in penalties reaching EUR 10 million or 2% of annual net turnover, depending on the severity of the breach.

Impact on the life sciences sector

To comply with Slovak NIS2 requirements, healthcare organisations should focus on:

- Continuous risk assessment covering electronic health records and other internal systems.
- Technical safeguards, including encryption, secure configuration, backups, and continuous monitoring.
- Robust internal policies, addressing technical, organisational, and physical risks.

NIS2, Data Privacy, AI

Key developments to watch

The Slovenian Law on Information Security, in force since June 2025, transposes the **NIS2 Directive** by broadening the scope to additional sectors and replacing prior identification with a size-based rule that captures medium and large entities, while introducing the new categorisation of “essential” and “important” entities with differentiated supervision and sanctions.

It tightens baseline cybersecurity risk-management and incident-reporting duties, strengthens supply chain security, mandates notification to service recipients in certain cases, and empowers national authorities to audit, issue binding instructions and impose effective, proportionate and dissuasive fines.

Practically, entities must establish documented information security management systems and implement prescribed technical and organisational measures aligned with Article 21 NIS2, with self-registration and use of new national digital platforms for information exchange, while benefiting from the ability to adapt existing documentation to the new regime.

The law aligns overlapping regimes by carving out, for banking and financial market infrastructure, the NIS2 risk-management, reporting and enforcement chapters in favour of DORA, in line with Commission guidance on Article 4 NIS2, and adjusts the electronic communications code (ZEKom-2) to reflect NIS2’s repeal of Articles 40-41 and shift sectoral obligations into the new framework.

Impact on the life sciences sector

The law now in force brings much of the life sciences sector squarely within scope by treating health as a “highly critical” sector, expressly covering hospitals and other healthcare providers, EU reference laboratories, entities conducting medicines R&D, manufacturers of pharmaceutical substances and preparations (NACE C-21), wholesalers holding distribution authorisations, and, during public health emergencies, manufacturers of specified critical medical devices.

In addition, general manufacturers of medical devices and IVDs are captured as “other critical” manufacturers outside emergencies. In practice, a size-based rule applies, with large entities in Annex I categories generally treated as “essential” and medium-sized entities in those categories, and medium/large device manufacturers in Annex II, treated as “important”, with the distinction driving supervisory intensity and sanctions.

Smaller hospitals, laboratories or speciality manufacturers can still be designated where disruption would seriously affect public order, public security or public health, where they are sole providers, or due to national criticality criteria. In-scope entities must maintain a documented information-security management system and implement Article 21-type risk management measures, including governance and accountability, cryptography, application security and strengthened supply-chain security, with the option to adapt existing documentation rather than rebuild it. They are subject to the incident-reporting regime (early notification and follow-ups), use Commission implementing acts where applicable on report content and thresholds, and must notify service recipients of significant incidents and relevant cyber threats.

Operationally, entities come under oversight via self-registration, enabling targeted supervision, with differentiated compliance monitoring and enforcement between essential and important entities.

Product liability

Key developments to watch

Slovenia must implement the product liability directive by the end of 2026. So far, no proposal has been published.

NIS2, Data Privacy, AI

Key developments to watch

- No NIS2- or AI Act-equivalent regulation adopted.
- Draft law restricting use of “hostile” (Russia-linked) software.
- No tightening of data-privacy rules beyond existing GDPR-inspired framework.
- AI regulation remains at monitoring stage.

Impact on the life sciences sector

- Despite Ukraine’s EU-alignment trajectory, no horizontal or sector-specific regulation comparable to **EU NIS2** or the **AI Act** has been adopted or is imminent, including for healthcare and life sciences.
- The only material cybersecurity initiative targets **software developed or owned by Russian residents**. If adopted, the Government will approve a list of prohibited software, primarily banning its use in the **public sector**, with **indirect effects on private suppliers to public entities from 2030**.
- **Implication:** Life sciences companies supplying medical devices, digital solutions or maintenance services to **state or municipal purchasers** would need to ensure that neither their products nor embedded software rely on listed solutions. This is particularly relevant for **medical devices with embedded software** and IT-supported servicing.
- Ukraine’s data protection regime remains stable, with no announced healthcare-specific or AI-driven processing restrictions.
- Ukraine has not proposed binding AI-specific legislation and continues to monitor EU developments. At the same time, healthcare-focused lawmakers have expressed openness to proposals that would gradually align Ukrainian regulations with EU approaches, while also supporting the development of the rapidly growing domestic AI start-up ecosystem.
- **Implication:** AI-enabled medical technologies face no Ukraine-specific regulatory burden in the near term; preparedness for the EU AI Act remains the primary compliance driver.

Market access and reimbursement

Key developments to watch

- Ukraine introduced regional & local budget pooling for **Managed Entry Agreements (MEAs) via Cabinet of Ministers Resolution No. 1704 (2025).**
- **HTA formally operationalised for medical devices.**
- Another expansion of the **outpatient reimbursement programme for medicines and medical devices for 2026.**
- **Increased use of confidential MEAs, including outcome-based agreements.**
- **Tightening of the price regulation framework** (National Price Catalogue and reference pricing).

Impact on the life sciences sector

Significantly increased purchasing power through pooling of state, regional, municipal and public-hospital budgets coordinated by the centralised medical procurement agency (MPU).

Strategic implications

- Accelerated access to innovative, high-cost therapies beyond the limits of the central state budget.
- Companies should proactively engage regional/local health authorities and public hospitals to secure co-funding commitments.
- MEA proposals can be designed around multi-budget funding structures, with flexible volumes and phased roll-out.

Medical devices HTA becomes actionable, while remaining voluntary. It is aligned with EU methodology and expected to influence public procurement and NHS of Ukraine decisions from 2026 onwards, particularly for higher-risk/higher-cost devices.

Strategic implications

- Medium- and-high risk device manufacturers must prepare **HTA-ready evidence packages**, including clinical effectiveness, economic value and (where relevant) real-world evidence.
- Early HTA planning becomes important for successful market access and public procurement positioning.

CONTINUED

Market access and reimbursement (continued)

Impact on the life sciences sector

Broader outpatient coverage increases access to reimbursed outpatient therapies, with growing relevance for chronic and long-term treatments (including cardiovascular, diabetes, lung diseases, oncology and mental health conditions).

In 2026, for the first time since the launch of the outpatient reimbursement programme in 2017, the Government has included several innovative therapies for which reimbursement will cover only 50% (in contrast to the full coverage or up to 10% co-payment for other therapies), with the remaining 50% payable out-of-pocket. In practice, this change introduces partial public funding for innovative therapies that were previously entirely paid out-of-pocket, thereby increasing their affordability.

MEAs are now a mainstream access tool for innovative therapies, including outcome-based models for oncology, rare diseases and other high-impact therapies.

Strategic implications

- Companies should be prepared to propose outcome-based or price-volume MEAs, supported by measurable endpoints and data-collection frameworks.
- There is a strong precedent for innovative therapies to enter the market via confidential pricing mechanisms rather than list-price routes.

Greater pricing discipline across the market, affecting both publicly funded (through reimbursement and procurement) and out-of-pocket products, including OTC.

Strategic implications

- Launch and lifecycle pricing strategies must carefully factor in reference pricing, declared prices and margin controls.

Anti-corruption and compliance

Key developments to watch

- **Good Promotional Practice** for medicinal products adopted: **(MOH Guideline ST-N MOHU 42-1.3:2025, June 2025).**
- **More active and visible regulatory compliance and anti-corruption enforcement.**
- **Closer supervision of market behaviour and regulatory engagement.**

Impact on the life sciences sector

- Introduces **clear, binding ethical standards** for interactions between pharmaceutical companies and healthcare professionals, aligned with **Directive 2001/83/EC**.
- **Implication:** Companies must review and update promotional policies, ensure transparency of HCP interactions, and align local practices with EU-level compliance standards.
- Enforcement activity has intensified, including investigations involving **pharmaceuticals, medical devices and public procurement**, with increased scrutiny of regulatory and market-surveillance bodies.
- **Implication:** Higher compliance risk in regulatory interactions, procurement processes and dealings with public authorities; companies should strengthen internal controls, approval processes and audit trails.
- The combination of EU-aligned promotional rules and stronger enforcement signals a **more structured and supervised compliance environment** for life sciences companies.
- **Implication:** Businesses should reassess compliance frameworks, monitor enforcement trends, and ensure robust governance over interactions with regulators, HCPs and public purchasers.

Product liability

Key developments to watch

- **No material changes to product liability regime.**
- **New Law on Consumer Rights Protection (expected).**

Impact on the life sciences sector

- Ukraine's product liability framework remains **unchanged**, with no significant current or forthcoming reforms specific to pharmaceuticals or medical devices.
- While a new law is expected to introduce general **consumer protection reforms**, it is **not anticipated to materially affect product liability rules** applicable to life sciences products. The legislative process should continue to be monitored.

Get in **touch**

WITH OUR

Life Sciences and Healthcare team

BIO

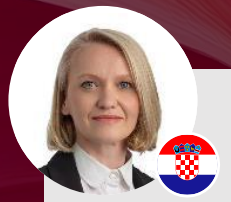
Gabriela Staber
Partner, Vienna
+43 1 40443 4850
gabriela.staber@cms-rrh.com

TEAM

Sanja Voloder
Counsel, Sarajevo
+387 33 94 4614
sanja.voloder@cms-rrh.com

BIO

Anna Tanova
Partner, Sofia
+359 2 921 9940
anna.tanova@cms-cmno.com



BIO

Marija Mušec
Partner, Zagreb
+385 1 4825 600
marija.musec@bmslegal.hr

BIO

Tomáš Matějovský
Managing Partner, Prague
+420 296 798 852
tomas.matejovsky@cms-cmno.com

BIO

Veronika Kovács
Partner, Budapest
+36 1 483 4878
veronika.kovacs@cms-cmno.com

BIO

Marija Filipovska Jelčić
Partner, Skopje
+389 2 3153 800
marija.filipovska-jelcic@cms-rrh.com

CONTINUED

Get in **touch**

WITH OUR

Life Sciences and Healthcare team

BIO

Agnieszka Starzynska
Partner, Warsaw
+48 22 520 84 58
agnieszka.starzynska@cms-cmno.com

BIO

Cristina Popescu
Partner, Bucharest
+40 21 407 3811
cristina.popescu@cms-cmno.com

BIO

Maja Stepanović
Partner, Belgrade
+381 11 3208900
maja.stepanovic@cms-rrh.com

BIO

Martina Gavalec
Partner, Bratislava
+421 2 3214 1424
martina.gavalec@cms-rrh.com

BIO

Robert Kordić
Senior Associate, Ljubljana
+386 1 438 4666
robert.kordic@cms-rrh.com

BIO

Borys Danevych
Co-Head of the CMS and CEE Head of Life Sciences & Healthcare, Kyiv
+38 044 391 3377
borys.danevych@cms-cmno.com

CMS Legal Updates subscription service

Sign up now for the free online email alert service delivering commentary, analyses and insights from CMS experts on the legal issues affecting your business, directly to your inbox.
cms.law/subscription

CMS locations:
Aberdeen, Abu Dhabi, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Bengaluru, Bergen, Berlin, Bogotá, Bratislava, Brisbane, Bristol, Brussels, Bucharest, Budapest, Casablanca, Chennai, Cologne, Dubai, Dublin, Duesseldorf, Ebene, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Gothenburg, Gurugram, Hamburg, Hong Kong, Hyderabad, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Maputo, Mexico City, Milan, Mombasa, Monaco, Mumbai, Munich, Muscat, Nairobi, New Delhi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, São Paulo, Sarajevo, Shanghai, Sheffield, Silicon Valley, Singapore, Skopje, Sofia, Stavanger, Stockholm, Strasbourg, Stuttgart, Sydney, Tel Aviv, Tirana, Vienna, Warsaw, Zagreb and Zurich.

Further information can be found at **cms.law**