Data Law Alert

Data Law



International Data Transfers and Cyber Resilience: New EU Developments

No.24 Issue 2026

Legance

ENISA's 2026 cybersecurity report highlights gaps in EU resilience

On **10 November 2026**, the European Union Agency for Cybersecurity ("**ENISA**") published the **2026 Report on the State of Cybersecurity in the Union**, adopted in cooperation with the European Commission and the NIS Cooperation Group. This second biennial edition, prepared under Article 18 of Directive (EU) 2022/2555 ("**NIS2**"), covers July 2024-July 2026 unless otherwise specified. The report records progress alongside persistent risks: the EU's cybersecurity posture has improved, while the level of cyber threats remains substantial and preparedness is uneven.

The report's strategic "compass" identifies five priorities: (i) effective implementation of legislation; (ii) crisis response; (iii) critical-infrastructure resilience; (iv) supply-chain risks and cross-border dependencies; and (v) awareness, skills and education. **Regulatory compliance alone is not the whole resilience picture**: ENISA highlights legacy systems, operational continuity and gaps in information sharing and coordination. It also describes artificial intelligence as **accelerating vulnerability discovery and exploitation**, while changing the skills cybersecurity teams need.

The report is an **institutional assessment and policy reference, not a new source of binding duties for businesses**. Its recommendations do not automatically become mandatory controls or a standalone test of NIS2 compliance: for **essential** and **important** entities, Articles 20 and 21 NIS2 remain the starting point for management oversight and proportionate risk-management measures, including supply-chain security, business continuity and training. Compliance must be assessed against the applicable legal requirements, not the report alone.

As a practical follow-up, businesses can **test documented risk assumptions against ENISA's findings**, review critical supplier dependencies and check incident procedures across providers and borders. Skills plans should reflect changing tasks and AI-related expertise. For identified gaps, businesses can assign owners, set remediation dates and report progress to management.

EDPB endorses Council of Europe and Ibero-American model clauses

On **10 November 2026**, the European Data Protection Board ("**EDPB**") adopted **Statement 3/2026 – on the use of other models of contractual clauses for onward transfers of personal data** – endorsing a European Commission clarification on onward transfers: situations in which an initial recipient passes personal data to another organization. Where the initial transfer uses the EU Standard Contractual Clauses ("**EU SCCs**"), the EU's pre-approved contractual safeguards for transfers outside the European Economic Area, the recipient may use Council of Europe or Ibero-American Data Protection Network ("**RIPD**") model clauses for the next transfer.

This is not a general replacement for the EU SCCs: the initial recipient must remain able to meet its original obligations, including using data only for the agreed purposes and cooperating with supervisory authorities. Furthermore, the **same protection** must continue for sensitive data, including criminal-offence data, together with any specific safeguards agreed in the original contract.

Controllers decide why and how personal data are processed; processors process data on their instructions. Both sets of model clauses cover **transfers between controllers and from a controller to a processor**. Council of Europe clauses also cover a processor passing data to another provider acting on its behalf, known as a **sub-processor**. If a later recipient sends the data to another country relying on a finding under local law that the destination provides adequate protection, **that transfer must also be covered by a European Commission decision recognising adequate protection**. Other routes must preserve the original EU SCC safeguards.

For these transfer arrangements, businesses must still assess whether relevant laws and practices in the destination country could prevent compliance with the EU SCCs: this is the **transfer impact assessment**. Additional safeguards are needed where gaps are identified; transfers must be suspended if adequate safeguards cannot be ensured.

Businesses should **map the full data-sharing chain**, choose clauses matching each party's role and check that the original safeguards remain effective. Contracts should keep cooperation, audit access and individuals' rights workable throughout the chain.

Data Law Alert

Data Law



For further information, please contact:

Andrea Fedi
afedi@legance.it

Lucio Scudiero
lscudiero@legance.it

Martina Balzani
mbalzani@legance.it