European Union & Member-State Vendor-Risk Guides

How Cyber Crucible supports EU-wide regimes (GDPR, DORA, NIS2, the AI Act) and member-state specifics (Germany, France, Ireland, Netherlands, Spain, Italy, Poland, Sweden) from a vendor-selection perspective. States plainly what Cyber Crucible holds and does not hold, and makes no compliance promises on the customer's behalf.

Which EU rules affect selecting a security vendor, beyond GDPR?

Short answer: Beyond the GDPR, three EU regimes increasingly shape vendor selection: DORA (operational resilience for financial entities and their ICT providers), NIS2 (cybersecurity obligations for essential and important entities, including supply-chain security), and the EU AI Act (risk-tiered rules for AI systems). Each pushes obligations toward vendors. Cyber Crucible's design — no customer content collected, local processing, on-premises option — supports a customer's obligations under all of them, without Cyber Crucible claiming compliance on the customer's behalf.

The landscape at a glance

- **GDPR** — the baseline for personal-data processing across the EU. See the Country Compliance Guides for the GDPR page.
- **DORA** — applies from 17 January 2025 to financial entities and, importantly, to their ICT third-party service providers.
- **NIS2** — member states were to transpose it by October 2024; as of 2026 most have, while several were still finalizing national law.
- **EU AI Act** — risk-tiered obligations phasing in through 2026–2027.

How Cyber Crucible fits

The recurring theme is supply-chain and third-party risk. Because Cyber Crucible collects no customer content, credentials, or keys and can run entirely within the customer's boundary, it reduces the surface these regimes are written to control. The pages in this book address each regime and the larger member states. Documentation is available from **dpo@cybercrucible.com**.

How does Cyber Crucible support EU financial entities under DORA?

Short answer: Cyber Crucible is an ICT third-party service provider in DORA terms, and it supports a financial entity's DORA obligations — contractual controls, incident information, and resilience testing — while reducing ICT third-party risk because it never collects the entity's data. DORA applies from 17 January 2025. Cyber Crucible does not claim to be "DORA compliant" on a customer's behalf; compliance is the financial entity's, and Cyber Crucible supplies the support and evidence its program needs.

How it supports the entity's DORA program

- **ICT risk reduction.** No customer content, credentials, or keys are collected, and protection runs locally — shrinking the third-party attack surface DORA targets.
- **Contractual controls.** Cyber Crucible can accommodate the contractual provisions DORA expects for ICT third-party arrangements (security, incident cooperation, audit and information rights, subcontracting transparency).
- **Incident cooperation.** A documented breach-response process provides prompt, evidence-grade information, and a committed notification timeframe is available by contract to support the entity's incident-reporting duties.
- **Resilience.** Endpoint protection continues during a management-backend outage, which supports operational-resilience objectives.

The honest boundary

DORA also allows the European Supervisory Authorities to designate **critical** ICT third-party service providers (CTPPs) for direct EU oversight. Cyber Crucible is not designated as a CTPP and does not represent itself as one. It supports the financial entity's obligations; it does not assume them.

How does Cyber Crucible support NIS2 obligations for essential and important entities?

Short answer: For an organization classified as an essential or important entity under NIS2, Cyber Crucible supports the required risk-management measures — endpoint protection, access control, encryption, and incident handling — and supports the directive's supply-chain-security expectations because it collects no customer data and can run inside the entity's boundary. Cyber Crucible supports these obligations; it does not certify or assume them.

How it supports NIS2 measures

- **Cybersecurity risk-management measures.** Autonomous endpoint prevention, MFA-backed access, and encryption map to several of the directive's baseline measures.
- **Supply-chain security.** As a supplier that collects no customer content and offers on-premises deployment, Cyber Crucible reduces rather than adds to the supply-chain risk NIS2 asks entities to manage.
- **Incident handling and reporting support.** A documented breach-response process helps the entity meet NIS2's early-warning and notification timelines.

The honest boundary

NIS2 obligations rest with the essential or important entity, not with an individual security tool. Member-state transposition varied: by 2026 most states had transposed the directive into national law, while several — including France, Ireland, the Netherlands, and Spain — were still finalizing it. Cyber Crucible holds no NIS2 "certification"; it supplies supporting control evidence under NDA.

How does Cyber Crucible relate to the EU AI Act?

Short answer: Cyber Crucible uses AI only during development (its Genetic AI discovery work) and runs fixed, deterministic heuristics at runtime — there is no live AI model making decisions on the customer's endpoint. So Cyber Crucible does not place a high-risk or general-purpose AI system into the customer's environment. The customer remains responsible for assessing its own obligations under the EU AI Act, whose requirements are phasing in through 2026–2027.

Why the architecture matters here

- **No runtime AI system deployed to the customer.** The endpoint runs deterministic kernel heuristics, not a live model — so there is no on-device AI system for the customer to classify and govern under the Act.
- **Development-time only.** The AI work happens in Cyber Crucible's internal development environment, on internal research datasets; no customer content, credentials, or keys are used to train, feed, or tune a model.
- **Transparency.** Because runtime behavior is deterministic and testable rather than probabilistic, it is straightforward to describe and document.

The honest boundary

Cyber Crucible does not claim the product is "EU AI Act compliant," and it does not make that determination for a customer. This page describes how the product works so a customer's own AI Act assessment can account for it accurately. This is not legal advice.

How does Cyber Crucible support data protection and security requirements in Germany?

Short answer: In Germany, Cyber Crucible supports an organization's obligations under the GDPR and the Federal Data Protection Act (BDSG) by collecting no customer content, credentials, or keys and processing on the endpoint. For organizations in scope of Germany's cybersecurity regime (the BSI Act framework, as it takes on NIS2), the local-processing, on-premises-capable design supports their security and supply-chain obligations.

How it aligns

- **GDPR + BDSG.** Data minimization, encryption, and access control support the German data-protection baseline; a data processing agreement is available.
- **Data residency.** On-premises deployment keeps personal data in Germany where required; no customer content is transferred offshore for security processing.
- **Cybersecurity regime.** Germany has been transposing NIS2 into its BSI Act framework; Cyber Crucible supports covered entities' risk-management and supply-chain measures.

The honest boundary

Compliance rests with the organization and, where relevant, its data protection officer and the competent supervisory authority. Cyber Crucible holds no German certification and supports, rather than assumes, these duties. Documentation is available on request.

How does Cyber Crucible support data protection requirements in France?

Short answer: In France, Cyber Crucible supports an organization's obligations under the GDPR and the Loi Informatique et Libertés (enforced by the CNIL) by minimizing data and processing locally. Because it collects no customer content, credentials, or keys, most obligations the CNIL enforces have minimal surface in its custody.

How it aligns

- **GDPR + national law.** Encryption, access control, and data minimization support the French baseline; a data processing agreement is available.
- **Data residency.** On-premises deployment keeps personal data in France where required.
- **Cybersecurity regime.** France's NIS2 transposition was still moving through the legislative process as of 2026; Cyber Crucible supports covered entities' security and supply-chain measures under the framework as adopted.

The honest boundary

The CNIL is an active supervisory authority; compliance is the organization's, and Cyber Crucible supports it without claiming a French certification. Documentation is available on request.

How does Cyber Crucible support data protection requirements in Ireland?

Short answer: In Ireland, Cyber Crucible supports an organization's obligations under the GDPR and the Data Protection Act 2018 (enforced by the Data Protection Commission) by collecting no customer content, credentials, or keys and processing on the endpoint. Ireland is the lead supervisory authority for many multinationals, which raises the bar for vendor scrutiny; the minimal data footprint keeps the vendor side low-risk.

How it aligns

- **GDPR + DPA 2018.** Data minimization, encryption, and access control support the Irish baseline; a data processing agreement is available.
- **Data residency.** On-premises deployment keeps personal data in Ireland where required.
- **Cybersecurity regime.** Ireland's NIS2 transposition was still being finalized as of 2026; Cyber Crucible supports covered entities' measures under the framework as adopted.

The honest boundary

The Data Protection Commission is a prominent lead authority in the EU; compliance is the organization's. Cyber Crucible holds no Irish certification and supports these duties. Documentation is available on request.

How does Cyber Crucible support data protection requirements in the Netherlands?

Short answer: In the Netherlands, Cyber Crucible supports an organization's obligations under the GDPR and the Dutch GDPR Implementation Act (enforced by the Autoriteit Persoonsgegevens) by minimizing data and processing on the endpoint. It collects no customer content, credentials, or keys, so most obligations have little surface in its custody.

How it aligns

- **GDPR + national implementation.** Encryption, access control, and data minimization support the Dutch baseline; a data processing agreement is available.
- **Data residency.** On-premises deployment keeps personal data in the Netherlands where required.
- **Cybersecurity regime.** The Netherlands' NIS2 transposition (the Cyberbeveiligingswet) was still being finalized as of 2026; Cyber Crucible supports covered entities' measures under the framework as adopted.

The honest boundary

Compliance rests with the organization and the Autoriteit Persoonsgegevens where relevant. Cyber Crucible holds no Dutch certification and supports these duties. Documentation is available on request.

How does Cyber Crucible support data protection requirements in Spain?

Short answer: In Spain, Cyber Crucible supports an organization's obligations under the GDPR and the Organic Law on Data Protection (LOPDGDD, enforced by the AEPD) by collecting no customer content, credentials, or keys and processing locally. Because there is minimal personal data in its custody, most obligations the AEPD enforces have little to attach to.

How it aligns

- **GDPR + LOPDGDD.** Data minimization, encryption, and access control support the Spanish baseline; a data processing agreement is available.
- **Data residency.** On-premises deployment keeps personal data in Spain where required.
- **Cybersecurity regime.** Spain's NIS2 transposition was still in the legislative process as of 2026; Cyber Crucible supports covered entities' measures under the framework as adopted.

The honest boundary

The AEPD is one of the EU's more active enforcers; compliance is the organization's. Cyber Crucible holds no Spanish certification and supports these duties. Documentation is available on request.

How does Cyber Crucible support data protection requirements in Italy?

Short answer: In Italy, Cyber Crucible supports an organization's obligations under the GDPR and the Italian Privacy Code (enforced by the Garante) by minimizing data and processing on the endpoint. It collects no customer content, credentials, or keys, so most obligations have minimal surface in its custody.

How it aligns

- **GDPR + Privacy Code.** Encryption, access control, and data minimization support the Italian baseline; a data processing agreement is available.
- **Data residency.** On-premises deployment keeps personal data in Italy where required.
- **Cybersecurity regime.** Italy was among the earlier member states to transpose NIS2 into national law; Cyber Crucible supports covered entities' risk-management and supply-chain measures.

The honest boundary

The Garante is an active supervisory authority; compliance is the organization's. Cyber Crucible holds no Italian certification and supports these duties. Documentation is available on request.

How does Cyber Crucible support data protection requirements in Poland?

Short answer: In Poland, Cyber Crucible supports an organization's obligations under the GDPR and the Polish Personal Data Protection Act (enforced by the UODO) by collecting no customer content, credentials, or keys and processing on the endpoint. The minimal data footprint keeps most obligations low-surface.

How it aligns

- **GDPR + national law.** Data minimization, encryption, and access control support the Polish baseline; a data processing agreement is available.
- **Data residency.** On-premises deployment keeps personal data in Poland where required.
- **Cybersecurity regime.** Poland has been updating its National Cybersecurity System (KSC) framework to reflect NIS2; Cyber Crucible supports covered entities' measures under the framework as adopted.

The honest boundary

Compliance rests with the organization and the UODO where relevant. Cyber Crucible holds no Polish certification and supports these duties. Documentation is available on request.

How does Cyber Crucible support data protection requirements in Sweden and the Nordics?

Short answer: In Sweden and the wider Nordic region, Cyber Crucible supports an organization's obligations under the GDPR and national implementing laws (in Sweden, enforced by the IMY) by minimizing data and processing on the endpoint. Because it collects no customer content, credentials, or keys, most obligations have little surface in its custody.

How it aligns

- **GDPR + national implementation.** Encryption, access control, and data minimization support the Nordic baseline; a data processing agreement is available.
- **Data residency.** On-premises deployment keeps personal data in-country where required.
- **Cybersecurity regime.** Nordic member states have been transposing NIS2 into national law on their own timelines; Cyber Crucible supports covered entities' measures under the framework as adopted.

The honest boundary

Compliance rests with the organization and the relevant national supervisory authority. Cyber Crucible holds no national certification in any Nordic country and supports, rather than assumes, these duties. Documentation is available on request.