Overview of Key EU Digital Regulations

part of our "Data & AI Coordinator Handbook"

Relevancy for Swiss companies

F Form
C Checklist
T Template
V Video Training

What is the regulation about and when is it relevant to us?	What are the main obligations for us?

AI Act

Regulates AI systems placed on the market, put into service, or whose output is used in the EEA. It adopts a risk-based approach to safeguard health, product safety, and fundamental rights. It classifies AI systems by risk: **prohibited practices** are banned outright; **high-risk systems** face extensive compliance requirements; **general-purpose AI models (GPAI)**, especially those with systemic risk, have specific obligations; and **other "limited-risk" AI systems** like chatbots are primarily subject to transparency obligations.

Artificial Intelligence (AI) refers to computer systems trained - not explicitly programmed - to recognize patterns and generate outputs, such as predictions, content, recommendations, or decisions. AI's key feature is autonomy: outputs arise from learned patterns in training data, not from fixed human-written rules. An ***AI system*** is any tool, online service, or application based on AI techniques.

Relevant to us if we:

- Place AI systems on the EEA market or put them into service in the EEA under our own name (**providers**).
- Deploy/use AI systems under our authority in the EEA (**deployers**).
- Distribute AI systems on the EEA market (**distributors**).
- Import AI systems or products embedding AI systems into the EEA (**importers**) or place such products on the EEA market under our own name (**manufacturers acting as providers**).

For Swiss companies: Same as above for EEA companies, but for the second scenario, relevant insofar as the output of our AI system is intended for use in the EEA. However, it is not applicable to a Swiss-based user whose AI system output is randomly and unintentionally used in the EEA.

Further reading & materials: vischer.com/ai

F C T V

As providers or deployers, we shall:

- **Avoid Prohibited AI Practices:** Not develop, market, or deploy AI systems for purposes that are prohibited under the AI Act, such as social scoring, exploiting human vulnerabilities, or emotion recognition in the workplace.
- **Manage High-Risk AI:** As providers placing "high risk" AI systems on the EEA market (such as those used in recruitment, credit scoring, or as product safety components), follow strict rules. These include implementing a risk management framework, maintaining high-quality data governance, enabling human oversight, keeping technical documentation, and ensuring that a conformity assessment is completed before release.
- **Ensure Transparency:** For other AI systems that interact with individuals, generate synthetic content, or perform emotion recognition or biometric categorization, ensure transparency. Users must be informed when interacting with an AI system (e.g., a chatbot), and AI-generated audio, images, videos, or texts ("deepfakes") must be clearly labeled as machine-generated.
- **Check Supplier Compliance:** When procuring or integrating third-party AI systems or components, ensure that suppliers comply with the AI Act's requirements through contracts.

Survival kit:

- Generative AI Risk Assessment Toolkit (GAIRA Toolkit)
- Template for an Inventory of AI Systems
- Checklist on AI for Contracts with Suppliers and Partners
- Checklist on Key AI Compliance Issues
- Questions to Determine the Applicability of the AI Act to Our Use Case
- AI Training Video for Employees (5 min., available in D/F/E)
- AI Policy (one-page or comprehensive form)

Data Act

Regulates access to, and sharing of, data from *"connected products"* and associated *"related services"*. Users have the right to freely access data from their use and share it with third parties on request, subject to safeguards such as the protection of trade secrets. *"Data holders"* (e.g., manufacturers, service providers) must design products/services to allow for data access, provide pre-contractual information, refrain from imposing unfair contractual terms, and facilitate switching between data processing services (e.g., cloud providers).

A ***connected product*** is hardware or software that obtains, generates, or collects data concerning its use or environment and is able to communicate that data digitally (e.g., smart home devices, fitness trackers, industrial machinery). A ***related service*** is a digital service functionally linked to a connected product's operation or features, and without which the product cannot perform one or more of its functions (e.g., control apps).

Relevant to us if we:

- Manufacture, import, or distribute connected products for the EEA market (**manufacturers acting as data holders**).
- Provide related services for connected products used within the EEA (**service providers acting as data holders**).
- Are otherwise considered a "data holder" under the Data Act by having the right or obligation to make data from connected products or related services available to users or data recipients in the EEA (**other data holders**).
- Act as providers of data processing services (e.g., cloud) to customers in the EEA, subject to Chapter VI switching rules (**other providers**).

For Swiss companies: Same as above for EEA companies.

T V

As data holders, we shall:

- **Enable User Data Access:** Upon a user's request, provide access to their product/related service data without undue delay, free of charge, and in a structured, commonly used, and machine-readable format.
- **Provide Pre-Contractual Information:** Before a contract is signed, clearly inform users about the type, format, and estimated volume of data that will be generated, how they can access it, and our intended use of the data.
- **Conclude Contract for Data Use:** To use a user's non-personal data for our own purposes (e.g., service improvement), conclude a specific agreement with the user.
- **Support Third Party Data Sharing:** Upon a user's request, make their data available to a third party of their choice. Data sharing with third-party data recipients must be on fair, reasonable, and non-discriminatory terms.
- **Ensure Non-Discrimination:** Do not apply dissimilar conditions to comparable categories of data recipients, including our own affiliated companies, when providing data access.
- **Facilitate Switching of Data Processing Services:** Remove commercial, technical, and organizational obstacles for customers to switch to another provider or an on-premises system.
- **Design for Compliance:** Design products and services so that data is accessible to the user by default. Implement appropriate measures to protect trade secrets and ensure compliance with the GDPR.

Survival kit:

- Standard Data Act Amendment for GTCs
- Template Agreement Between Data Holder and Data User
- Template Agreement Between Data Holder and Data Recipient
- Template of a Pre-Contractual Information Notice

Cyber Resilience Act (CRA)

Establishes mandatory cybersecurity requirements for *"products with digital elements"* made available within the EEA, setting requirements for their secure design, development, production, and maintenance to reduce cyber risks across their lifecycle.

A ***product with digital element (PDE)*** is hardware or software that connects directly or indirectly to a network or device and may be exposed to cyber threats (e.g., browsers, routers, smartphones, password managers, fitness trackers, industrial control systems). Lifecycle activities include continuous vulnerability management, security updates, and incident reporting to ensure ongoing protection and resilience against cyberattacks.

Relevant to us if we:

- Manufacture any PDE for the EEA market (**manufacturers**).
- Import or distribute any PDE in the EEA (**importers/distributors**).

Note: A "connected product" under the Data Act is typically also a "product with a digital element" under the CRA (but not vice versa).

For Swiss companies: Same as above for EEA companies.

V

As manufacturers, we shall:

- **Implement Security by Design/Default:** Build cybersecurity requirements (e.g., no default passwords, access control, secure updates, encryption) into products from design through support.
- **Perform Conformity Assessment:** Conduct a cybersecurity risk assessment, develop technical docs, prove compliance with self/third-party evaluation, and affix the CE marking before market placement.
- **Report Incidents:** Notify ENISA of actively exploited vulnerabilities within 24h, followed by updates and a final report.
- **Manage Vulnerabilities:** Disclose vulnerabilities responsibly, deliver free security updates throughout the product's lifecycle (min. 5 years), and publish end-of-support dates.

As importers/distributors, we shall:

- **Verify & Monitor Compliance:** Ensure manufacturer obligations are met, retain the declaration of conformity and technical docs, verify the CE marking, cooperate with authorities, report risks, and withdraw or recall non-compliant products.
- **Include CRA clauses:** Include CRA compliance clauses in contracts with supply chain operators.

NIS2 Directive

Mandates a high common level of cybersecurity resilience for organizations operating in critical sectors across the EEA, classified as *"essential"* (e.g., energy, transport, finance, healthcare) and *"important"* (e.g., postal services, manufacturing of key products, digital infrastructure) entities.

Relevant to us if we:

- Operate in a regulated sector, meet size thresholds (≥50 employees or >€10M turnover), and provide services in the EEA.
- Supply products or services to in-scope entities, as NIS2 requirements may extend through supply chain security clauses or contractual obligations.
- Provide cross-border network or digital services (e.g., managed ICT, cloud hosting) to customers based in the EEA.
- Are designated by an EEA Member State despite our small size due to systemic cyber risk.
- Serve as B2B digital providers (e.g., marketplaces, search engines).

For Swiss companies: Same as above for EEA companies (except for the first scenario), and we need an EEA representative.

As essential or important entities, we shall:

- **Register & Appoint a Representative:** Register with national authorities; appoint an EEA representative if based outside the EEA.
- **Manage Cyber Risks:** Implement a comprehensive cybersecurity risk management (risk analysis, incident handling, business continuity, access control, encryption, and vulnerability management).
- **Secure the Supply Chain:** Assess and mitigate cybersecurity risks associated with suppliers and service providers through contracts.
- **Report Incidents:** Notify the CSIRT within 24h (early warning), provide a detailed report within 72h, and a final report within 1 month; inform affected customers.
- **Ensure Management Oversight:** Have senior executives approve, oversee, train on, and be accountable for cybersecurity measures.

As suppliers to in-scope entities, we shall:

- **Verify & Document Compliance:** Meet customer cybersecurity requirements, including risk management, incident-response capabilities, and documented security evidence (e.g., audit records).
- **Report Upstream:** Notify customers of incidents within stipulated timelines.

Digital Services Act (DSA)

Regulates online intermediary services offered in the EEA to combat illegal content and enhance transparency. Obligations are tiered according to service type, ranging from basic intermediaries and hosting providers to online platforms, including very large online platforms.

Relevant to us if we:

- Provide internet access services (e.g., public Wi-Fi networks) in the EEA.
- Offer caching services (e.g., content delivery networks) in the EEA.
- Provide hosting services (e.g., cloud storage, web hosting, SaaS that stores customer-generate content) in the EEA.
- Operate online platforms enabling public user-generated content (e.g., marketplaces, social media, app stores, forums) in the EEA.

Note: Simple company websites or online shops without user-generated content are not in scope.

For Swiss companies: Same as above for EEA companies, and we need an EEA representative.

As in-scope providers of intermediary services, we shall:

- **Establish Points of Contact:** Appoint a single point of contact for authorities and users; appoint an EEA representative if based outside the EEA.
- **Report on Content Moderation:** Publish annual transparency reports on content moderation activities and decisions.
- **Disclose rules:** Clearly state content moderation policies in the terms and conditions.

As hosting providers, we shall additionally:

- **Enable Illegal Content Reporting:** Provide a notice-and-action mechanism for illegal content reports.

As online platforms, we shall additionally:

- **Provide a Complaint Process:** Implement an internal complaint-handling system for content moderation decisions.
- **Design Fair Interfaces:** Avoid manipulative interfaces ("dark patterns").
- **Disclose Advertising and Recommender Systems:** Be transparent about advertising and the parameters used in recommender systems.

Digital Markets Act (DMA)

Regulates very large online platforms designated as *"gatekeepers"* (e.g., Google Search, Apple's App Store, Amazon Marketplace, Meta Messenger) to ensure fair digital markets and contestability. It primarily grants rights to businesses rather than imposing direct obligations.

Relevant to us if we:

- Use gatekeeper services to reach customers in the EEA (e.g., app stores, search engines, marketplaces).
- Benefit from rules that prevent self-preferencing, enforce data interoperability, and prohibit unfair or forced payment systems.
- Compete with gatekeepers in ancillary services (e.g., advertising, browser engines).

Note: Only applies to us if we are designated as a gatekeeper (unlikely unless we exceed the thresholds, i.e., EUR 7.5B EEA turnover + 45M monthly users).

For Swiss companies: Relevant mainly as business users of gatekeeper services in the EEA (we benefit from the DMA rights); direct obligations apply only if we are designated as a gatekeeper (unlikely).

As users of gatekeeper services, we shall (these are rights, not obligations):

- **Monitor Fair Access:** Track gatekeepers for self-preferencing, data barriers, or discriminatory terms affecting our business.
- **Claim Our Data:** Request access to aggregated data generated by our business activities on their platforms.
- **Ensure Equal Treatment:** Verify fair ranking in search results, app stores, and recommendations without favoritism.
- **Resist Bundling:** Reject the forced use of their payment systems, identity services, or ancillary products.
- **Demand Interoperability:** Require compatibility with third-party apps, browsers, messaging, and payment solutions.
- **Support Sideloading:** Expect alternative app distribution channels and anti-steering protections for users.
- **Access Real-Time Data:** Obtain live data feeds from gatekeeper platforms for our analytics or services.
- **Choose External Defaults:** Leverage user's ability to choose third party search engines or browsers as default.
- **Report Violations:** Escalate suspected DMA breaches to the European Commission or legal experts promptly.

Data Governance Act (DGA)

Aims to facilitate voluntary data sharing across the EEA through data intermediaries, public sector data reuse, and data altruism organizations. It mainly creates opportunities, while placing limited or role-specific obligations on businesses.

Relevant to us if we:

- Access or reuse public sector data in the EEA for commercial or research purposes (e.g., mobility, health, environmental data).
- Operate as neutral data intermediaries facilitating data sharing between private parties in the EEA.
- Participate in "data altruism" (voluntarily donating data for general interest purposes) in the EEA.

Note: Registration with national authorities is required if operating as a data intermediary or data altruism organization (these roles are voluntary to adopt).

For Swiss companies: Same as above for EEA companies.

As data users accessing public sector data, we shall:

- **Respect Data Conditions:** Comply with usage restrictions, licensing terms, and purpose limitations set by public sector bodies.
- **Report Usage:** Track and report data usage as required by licensing agreements.

As data intermediaries, we shall:

- **Register & Notify:** Notify national authorities before operating; maintain impartiality and transparency toward all parties.
- **Comply with Rules:** Ensure secure handling of data, refrain from monetizing data in breach of DGA principles, submit annual transparency reports, and manage user consent.

As data altruism organizations, we shall:

- **Register & Certify:** Register with the relevant national authority; obtain certification or recognition for general interest activities.
- **Operate Transparently:** Publish clear data use policies, ensure free and voluntary donations, protect donor rights, and maintain data security.

Authors: David Rosenthal, Samira Studer