Chambers AND PARTNERS

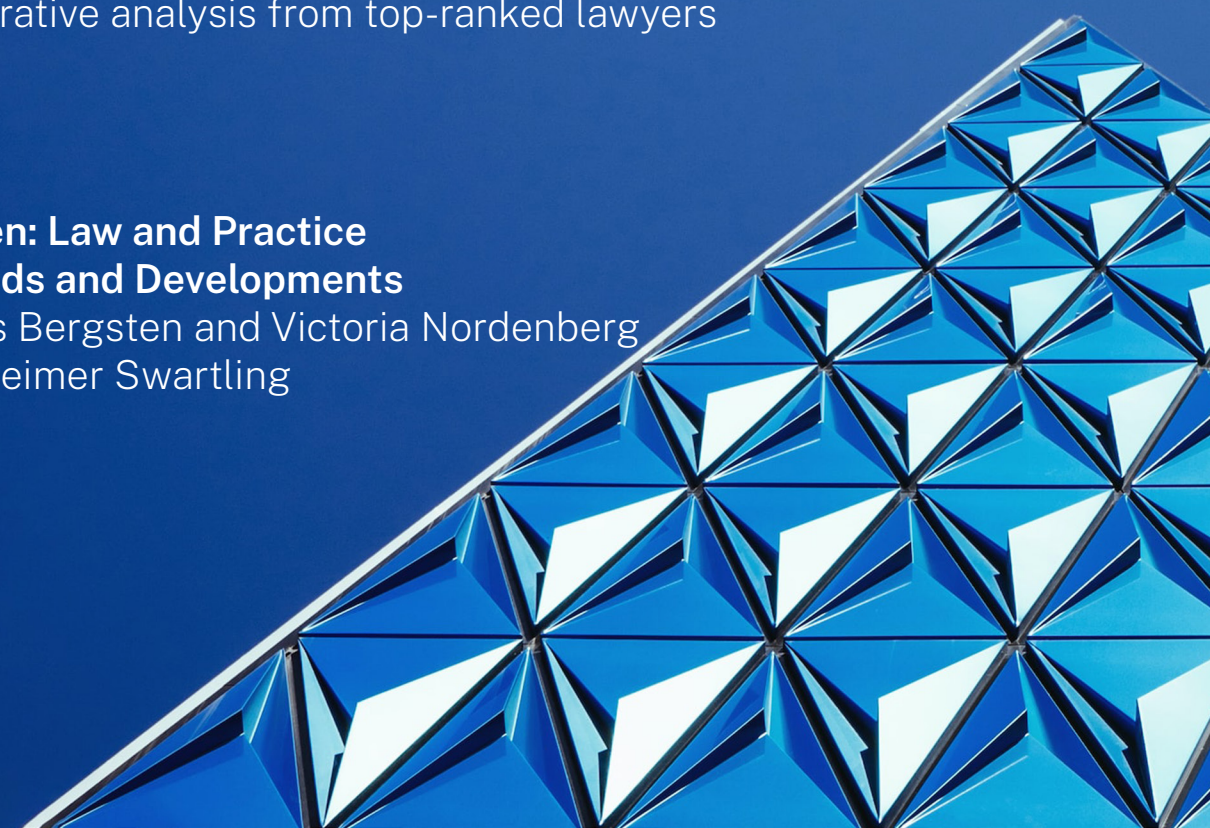
CHAMBERS GLOBAL PRACTICE GUIDES

# Cybersecurity 2025

Definitive global law guides offering comparative analysis from top-ranked lawyers

**Sweden: Law and Practice & Trends and Developments**

Anders Bergsten and Victoria Nordenberg
Mannheimer Swartling



# SWEDEN


## Law and Practice

**Contributed by:**
Anders Bergsten and Victoria Nordenberg
**Mannheimer Swartling**

## Contents

**Mannheimer Swartling** is the largest law firm in the Nordics and is a leading adviser in the premium segment for business law in Sweden. Its full-service practice is unique for Sweden in that the lawyers have a high degree of specialisation. The firm can therefore cover all the specialist advice needs of its clients – of any size or complexity – in-house. The corporate commercial team consists of 75 lawyers based in Stockholm, Gothenburg and Malmö. The team regularly acts on large IT procurements and outsourcings where complex cybersecurity issues arise. Cybersecurity matters within digitalisation projects, online currencies and collaboration agreements are also frequently handled by the team. Another strength is data protection mandates ranging from GDPR compliance to data breaches. Clients also benefit from the team's close collaboration with the M&A department to assist with technology-related set-ups. Clients from the healthcare, automotive and technology sectors mandate Mannheimer Swartling.

## Authors

**Anders Bergsten** is a member of Mannheimer Swartling's corporate, tech and IP practice group, and is based in Stockholm. He advises clients on a wide range of national and international commercial matters, focused on the IT and technology area. Anders' practice consists mainly of advising on complex delivery, outsourcing and procurement projects, together with advising on cybersecurity, protective security, digital compliance and personal data matters. Anders joined the firm in 2006 and is a member of the Swedish Bar Association. He has an LLM degree from the University of Uppsala and has studied law at the University of Sydney.

**Victoria Nordenberg** is a member of Mannheimer Swartling's corporate, tech and IP practice group. She advises Swedish and international clients across a wide range of industries, with a particular focus on societal functions and critical infrastructure. Victoria has extensive experience in drafting and negotiating IT contracts, outsourcing agreements and other complex commercial agreements. In addition, Victoria has significant experience working with cybersecurity and digital communications regulation. Victoria joined the firm in 2016 and is a member of the Swedish Bar Association. She holds an LLM degree from the University of Uppsala.

Mannheimer Swartling
Advokatbyrå AB

Norrlandsgatan 21
111 43
Stockholm
Sweden

Tel: +46 859 506 000
Fax: +46 859 506 001
Email: felicity.trocme@msa.se
Web: www.mannheimerswartling.se

## 1. General Overview of Laws and Regulators

### 1.1 Cybersecurity Regulation Strategy

Sweden's approach to cybersecurity regulation is characterised by a diverse array of legal frameworks tailored to the specific needs and risks of each sector. Historically, this sectoral approach has allowed for targeted cybersecurity measures that address the unique challenges faced by different industries.

In response to the deteriorating global security landscape and increasing digitalisation, Sweden has initiated several new measures to strengthen its cybersecurity posture and take a more comprehensive approach to cybersecurity. A key development is the formulation of a strategy that addresses the country's foreign and security policy in relation to cyber and digital issues. The main focus of Sweden's cybersecurity strategy and efforts is to prevent cyberattacks and build resilience against them. This includes protecting critical infrastructure and sensitive information while ensuring that the country can recover and adapt quickly in the face of cyber threats. By improving resilience, Sweden aims to maintain the integrity and security of its digital environment, thereby safeguarding its national interests and the well-being of its citizens.

Overall, Sweden aims to address transnational cyber threats more effectively and improve its overall resilience through regulation and by working with international partners, particularly within the European Union and NATO, with a focus on protecting national interests and promoting global security.

### 1.2 Cybersecurity Laws

- The Electronic Communications Act (*Lag (2022:482) om elektronisk kommunikation*) and the Electronic Communications Regulation (*Förordning (2022:511) om elektronisk kommunikation*) transpose the Directive of the European Parliament and of the Council (2018/1972) of 11 December 2018 establishing the European Electronic Communications Code (recast). The act and the regulation regulate electronic communications, with a focus on the security and integrity of networks and services. They ensure that communication providers implement measures to protect against cybersecurity threats.

- The Accounting Act (*Bokföringslagen (1999:1078)*) contains provisions on the secure handling and storage of financial data, which is crucial for cybersecurity in financial reporting.
- The Camera Surveillance Act (*Kamerabevakningslagen (2018:1200)*) regulates camera surveillance, balancing security needs with privacy rights, and ensuring that surveillance systems are secure against unauthorised access.
- The Protective Security Act (*Säkerhetsskyddslagen (2018:585)*) and the Protective Security Regulation (*Säkerhetsskyddsförordningen (2021:955)*) focus on protective security, and require organisations to protect information that concerns security-sensitive activities from cyber threats, thus playing an important role in the broader cybersecurity framework.
- The Information Security for Critical and Digital Services Act (*Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*) and the Information Security for Critical and Digital Services Regulation (*Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster*) transpose Directive of the European Parliament and of the Council (2016/1148) of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. The act and the regulation impose obligations on operators of essential services and digital service providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. See **2 Critical Infrastructure Cybersecurity**.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), sets the standard for data protection and privacy in the EU, and requires organisations to implement robust security measures to protect personal data. The Data Protection Act containing supplementary provisions to the GDPR (*Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning*) complements the GDPR by providing additional national rules for data protection in Sweden, ensuring comprehensive data security. See **6.1 Cybersecurity and Data Protection**.
- The Patient Data Act (*Patientdatalag (2008:355)*) and the Patient Data Regulation (*Patientdataförordning (2008:360)*) complement the GDPR and include regulations for handling personal data in the healthcare sector.
- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA) aims to enhance digital operational resilience within the financial sector by setting uniform requirements across the EU. See **3 Financial Sector Operational Resilience Regulation**.
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 ("Cybersecurity Act") establishes the European Union Agency for Cybersecurity (ENISA) and a framework for cybersecurity certification of ICT products, see **5.1 Key Cybersecurity Certification Legislation**.

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 ("AI Act") establishes rules for artificial intelligence, including security requirements for AI systems, to ensure they are safe and trustworthy. See **6.2 Cybersecurity and AI**.
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("eIDAS Regulation") governs electronic identification and trust services, ensuring secure electronic transactions across the EU and setting the standards for secure electronic signatures and transactions.

### 1.3 Cybersecurity Regulators

- The Electronic Communications Act and the Electronic Communications Regulation: The Swedish Post and Telecom Authority (PTS) is the supervisory authority of these laws. PTS ensures that communication providers maintain the security and integrity of their networks and services. Its scope includes supervision of communication providers.
- The Accounting Act: The Swedish Accounting Standards Board (BFN) is the supervisory authority, focusing on the secure handling and storage of financial data. Although primarily concerned with accounting practices, BFN's role includes ensuring that financial data is protected against unauthorised access.
- The Camera Surveillance Act: The Swedish Authority for Privacy Protection (IMY) is the supervisory authority under this act, balancing security needs with privacy rights. The supervision shall ensure that surveillance systems are secure against unauthorised access, protecting individuals' privacy while allowing for necessary security measures.
- The Protective Security Act and the Protective Security Regulation: The supervisory mandate is divided up according to the sector in which the supervised entity (referred to as "the operator") is active, and the following authorities are sharing the mandate: the Swedish Security Service, the Swedish Armed Forces, the Authority for Swedish Transmission System, the Swedish Transport Agency, PTS, the Swedish Defence Materiel Administration, the Swedish Financial Supervisory Authority, the Swedish Energy Agency, the Swedish Radiation Safety Authority, and the County Administrative Boards in Stockholm, Skåne, Västra Götaland and Norrbotten. The supervision shall ensure that the operators fulfil the obligations imposed and focus on protection of security sensitive activities from cyber threats. Their role is critical in safeguarding national security and ensuring the protection of critical infrastructure.
- The Information Security for Essential and Digital Services Act and the Information Security for Essential and Digital Services Regulation: The Swedish Civil Contingencies Agency (MSB) is the primary regulator, acting as a co-ordinator among sector-specific regulators and a national contact point in the EU co-operation regarding NIS. See **2 Critical Infrastructure Cybersecurity**.
- GDPR and the Data Protection Act: The Swedish Authority for Privacy Protection has the supervision mandate in Sweden. The Swedish Authority for Privacy Protection ensures that organisations implement robust security measures to protect personal data.

Their authority covers all personal data processing activities within Sweden.
- The Patient Data Act and the Patient Data Regulation: The Swedish Authority for Privacy Protection is the supervisory authority that supervises the application of data protection rules by healthcare providers, which means, for example, checking that healthcare providers take security measures to protect patient data.
- DORA: The Swedish Financial Supervisory Authority is the supervisory authority that ensures that financial entities comply with DORA.
- The Cybersecurity Act: The ENISA is the key regulator for this regulation. ENISA develops cybersecurity certification frameworks to enhance trust and security in the digital market. Their authority covers ICT products and services across the EU, promoting a common approach to cybersecurity certification.
- The AI Act: The European Commission also oversees this regulation, establishing rules for artificial intelligence systems. The AI Act includes security requirements to ensure AI systems are safe and trustworthy, which are integral to cybersecurity. Its scope covers AI systems and applications throughout the EU.
- The eIDAS Regulation: In Sweden, the Swedish Agency for Digital Government is responsible for implementing this regulation. The Swedish Agency for Digital Government oversees electronic identification and trust services, ensuring secure electronic transactions.

## 2. Critical Infrastructure Cybersecurity

### 2.1 Scope of Critical Infrastructure Cybersecurity Regulation

Note that when Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2) is transposed into Swedish law, it will replace the current regulations.

#### Scope of Application

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS) was implemented in Sweden through the Act on Information Security for Critical and Digital Services and the Regulation on Information Security for Critical and Digital Services. The legislation entered into force on 1 August 2018. The purpose of the legislation is to enhance the security level of network and information systems for digital services and essential services within certain sectors. Operators covered by the regulatory framework are categorised into:

- operators of essential services, and
- digital service providers.

#### Operators of Essential Services

Operators of essential services exist in both private and public sectors. An operator of essential services is defined as an entity that:

- provides a service crucial for maintaining critical societal or economic activities within one of the seven sectors listed below:
  (a) energy;

(b) transport;
(c) banking;
(d) financial market infrastructure;
(e) healthcare;
(f) drinking water supply and distribution; or
(g) digital infrastructure;

- the provision of such service depends on network and information systems; and
- an incident would cause a significant disruption in the provision of the service.

### Digital Service Providers

Digital service providers exist in both private and public sectors. A digital service provider is defined as an entity that:

- has its main establishment in Sweden;
- has an annual turnover exceeding EUR10 million; and
- has 50 or more employees.

## 2.2 Critical Infrastructure Cybersecurity Requirements

### Obligations for Operators of Essential Services

An operator of essential services shall:

- conduct systematic and risk-based information security work concerning the network and information systems used to deliver the essential services;
- conduct a risk analysis that will serve as the basis for selecting security measures;
- implement appropriate and proportionate technical and organisational measures to manage risks threatening the security of the network and information systems used to provide the essential services; and
- take appropriate measures to prevent and minimise the impact of incidents affecting the network and information systems used to provide the essential services.

### Obligations for Providers of Digital Services

A provider of digital services shall:

- implement the technical and organisational measures considered appropriate and proportionate to address risks threatening the security of the networks and information systems used in the provision of digital services within the European Union; such measures should ensure a level of security in the network and information systems that is appropriate to the risk; and
- take measures to prevent and minimise the impact of incidents affecting the network and information systems used; these measures should aim at ensuring the continuity of services.

## 2.3 Incident Response and Notification Obligations

### Notification Requirements

Operators of essential services and providers of digital services are required to report any incidents that occur. This contributes to creating a comprehensive view of the incident situation, enables warnings to others, and facilitates any necessary co-ordinated efforts.

Reports are submitted to the Swedish Civil Contingencies Agency, which has a co-ordinating role for the Information Security for Critical and Digital Services Act, which forwards the reports to the respective supervisory authority. The Swedish Civil Contingencies Agency has announced regulations and general advice on incident reporting for providers of essential services.

The Swedish Post and Telecom Authority is the supervisory authority for providers of digital services.

The following authorities are, for the specified sectors, the supervisory authority for operators of essential services:

- Swedish Energy Agency: energy;
- Swedish Transport Agency: transport;
- Swedish Financial Supervisory Authority: banking;
- Swedish Financial Supervisory Authority: financial market infrastructure;
- Health and Social Care Inspectorate: healthcare;
- Swedish Food Agency: drinking water supply and distribution; and
- Swedish Post and Telecom Authority: digital infrastructure.

### 2.4 State Responsibilities and Obligations

CERT-SE is Sweden's national CSIRT (Computer Security Incident Response Team) tasked with supporting society in managing and preventing IT incidents. CERT-SE is part of the Swedish Civil Contingencies Agency, which helps integrate their efforts into the broader national security framework.

CERT-SE's responsibilities include providing assistance and guidance to the public sector, private companies, and organisations in handling cybersecurity threats and incidents. They aim to enhance the overall cybersecurity posture by offering expertise, co-ordinating responses to incidents, and promoting best practices for IT security.

## 3. Financial Sector Operational Resilience Regulation

### 3.1 Scope of Financial Sector Operational Resilience Regulation

In Sweden, the scope of financial sector operational resilience regulation is primarily governed by DORA. This regulation applies to a wide range of financial entities, including (but not limited to) banks, credit institutions, payment institutions, insurance companies, and alternative investment fund managers. DORA aims to enhance digital operational resilience by setting uniform requirements across the EU, and it is directly applicable in Sweden, requiring national legislation to complement it. The regulation excludes certain small entities and those covered by specific exemptions.

### 3.2 ICT Service Provider Contractual Requirements

#### Contractual Requirements

Under the framework of DORA, contractual requirements for ICT service providers include clear terms on service levels, security measures, data protection, incident management, and termination rights. Contracts must also include provisions for audit rights and access to information necessary for the financial institution to comply with its regulatory obligations under DORA.

#### ICT Service Providers

In Sweden, under the framework of DORA, "ICT service providers" are defined broadly to encompass entities that offer information and communication technology services to financial institutions. These include a wide range of services such as cloud computing, data analytics, software development, and cybersecurity services. The definition is intended to cover any third-party service that could impact the operational resilience of financial entities.

### Critical ICT Services

Not all ICT services are classified as critical. The classification of an ICT service as critical depends on several factors, such as the systemic impact of a failure in providing the ICT services, the reliance of financial entities, the degree of substitutability and other relevant factors. While the definition of ICT service providers in Sweden is broad, the classification of services as critical is specific and based on the potential impact on financial operations and stability.

### Cloud Service Providers

Not every cloud service provider will automatically be classified as critical. The criticality of a cloud service provider is assessed based on the same criteria mentioned above. For instance:

- If a cloud service provider supports a significant portion of a financial entity's operations or hosts critical applications, it may be classified as critical.
- Cloud service providers offering infrastructure as a service (IaaS) or platform as a service (PaaS) that are integral to the financial entity's operations are more likely to be considered critical compared to those offering less essential services.

## 3.3 Key Operational Resilience Obligations

### Objectives

The Swedish implementation of DORA is designed to ensure that financial entities can withstand, respond to, and recover from ICT-related disruptions, thereby enhancing their resilience. It also seeks to establish a unified framework for managing ICT risks across the financial sector, standardising risk management practices. By improving incident response, the regulation ensures that financial entities can respond to ICT incidents in a timely and effective manner, minimising their impact. Additionally, the regulation facilitates supervision by enabling effective oversight by regulatory authorities to ensure compliance and resilience.

### Key Obligations

Financial entities are required to implement comprehensive ICT risk management frameworks, which include regular risk assessments and mitigation strategies. They must also manage risks associated with ICT service providers, ensuring that contracts include necessary provisions for resilience and security. Regular testing and monitoring of digital operational resilience are required, including threat-led penetration testing for critical entities. Furthermore, clear governance structures for ICT risk management must be established, with defined roles and responsibilities.

### Incident and Reporting Obligations

Financial entities must classify ICT-related incidents based on their impact and severity. Significant incidents must be reported to the Swedish Financial Supervisory Authority within a specified timeframe, typically within 24 to 72 hours, depending on the severity. Reports should include details such as the nature of the incident, its impact, and the measures taken to address it. Entities are also required to conduct a post-incident analysis to identify root causes and implement measures to prevent recurrence. In certain cases, entities may be required to disclose incidents to the public, especially if they have a significant impact on customers or the financial system. It should be noted that entities that carry out operations covered by both DORA and the Protective Security Act must adhere to both in case of incidents, and that the incident reporting under DORA needs to take the obligations under the Protective Security Act into

consideration (which may curb the ability of an entity to report certain information under DORA).

## 3.4 Operational Resilience Enforcement

### Enforcement in Regard to Critical ICT Service Providers

The supervision of critical ICT service providers is to be carried out at Union level by the Lead Overseer. One of the three European Supervisory Authorities (European Banking Authority, European Securities and Markets Authority or European Insurance and Occupational Pensions Authority) is to be designated as Lead Overseer for each of the critical third-party service providers. In order to fulfil its tasks under DORA, the Lead Overseer may, inter alia, conduct general investigations and inspections. Within three months of the conclusion of an investigation or an inspection, the Lead Overseer shall adopt recommendations addressed to the critical third-party provider.

The Lead Overseer can impose a periodic penalty payment on the critical ICT service providers. Decisions on periodic penalty payments taken by the Lead Overseer should therefore be enforceable under the Swedish Enforcement Code (*Utsökningsbalken (1981:774)*) in the same way as a Swedish judgment that has acquired legal force. The Swedish Enforcement Authority (*Kronofogden*) is the Swedish authority that will be responsible for the practical enforcement and its decisions can be appealed to the Swedish court.

### Enforcement in Regard to Financial Entities

In regard to financial entities, the enforcement of operational resilience obligations is carried out by the Swedish Financial Supervisory Authority. The authority has the power to conduct inspections, request information, and impose sanctions or corrective measures on financial institutions and critical ICT service providers that fail to comply with operational resilience requirements. This includes fines, orders to cease certain activities, or other regulatory actions to ensure compliance.

## 3.5 International Data Transfers

There is no applicable information in this jurisdiction.

## 3.6 Threat-Led Penetration Testing

In Sweden, DORA mandates threat-led penetration testing (TLPT) for financial entities. These tests must be conducted every three years, or more frequently if required by the competent authority. The tests simulate cyber-attacks to identify vulnerabilities in an organisation's ICT infrastructure.

The tests must be executed by an external party every third time, while internal testers can be used but require specific approval and must meet conflict-of-interest requirements. The Swedish authorities, primarily the Swedish Financial Supervisory Authority and the Swedish Central Bank, share responsibilities for the TLPT process. The Swedish Financial Supervisory Authority determines which entities must undergo testing and the frequency of tests, while the Swedish Central Bank co-ordinates and monitors the tests, ensuring compliance and certifying that the tests meet the required standards. After completing the tests, entities must submit results, corrective action plans, and receive certification. This certification facilitates mutual recognition of tests across EU member states.

## 4. Cyber-Resilience

### 4.1 Cyber-Resilience Legislation

#### The EU Cyber Resilience Act

On 10 December 2024, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements ("Cyber Resilience Act") entered into force.

#### Implementation Timeline

Although the Cyber Resilience Act took effect on 10 December 2024, its full implementation is phased across three key dates: The main obligations introduced by the Cyber Resilience Act will apply from 11 December 2027, with the exception of Article 14 which will apply from 11 September 2026 and Chapter IV (Articles 35-51) which will apply from 11 June 2026.

#### The Inquiry Stage

On 28 November 2024, the Swedish government appointed an inquiry chair who will analyse the need for and propose measures and supplementary legislative provisions necessary to adapt Swedish law to the Cyber Resilience Act.

The work consists, inter alia, of identifying which provisions in Swedish legislation are affected by the Cyber Resilience Act and analysing whether they need to be repealed or amended, or if new provisions are needed as a result of the Cyber Resilience Act.

The investigator will, in particular:

- propose which existing authority or authorities should be designated as the national market surveillance authority;
- propose which existing authority should be designated as the notifying authority responsible for, among other things, establishing and implementing the procedures necessary for the assessment, designation, and notification of conformity assessment bodies; and
- make any other proposals, including legislative proposals, that are necessary or otherwise deemed appropriate to complement the Cyber Resilience Act.

The inquiry chair has to present its proposals in a report no later than 15 December 2025.

### 4.2 Key Obligations Under Legislation

#### Scope of Application

The Cyber Resilience Act applies to "products with digital elements" whose purpose or use involves a logical or physical data connection to a device or network.

The Cyber Resilience Act covers a wide range of software and hardware products that connect, either directly or indirectly, to other devices or networks. This includes smart home devices, wearable technology, internet-connected toys, and industrial Internet of Things (IoT) devices. Non-commercial open-source software products are not covered by the Cyber Resilience Act. The Cyber Resilience Act targets manufacturers, producers, and importers, requiring them to ensure that their products are safe to use, resilient to cyber threats, and that their security features are properly disclosed.

#### Objectives

The Cyber Resilience Act establishes compulsory cybersecurity standards for products with digital components available in the EU market.

Its primary objectives are to:

- improve the cybersecurity of digital products, from the design and development phase and throughout the whole life cycle;
- protect consumers and businesses against the risks posed by inadequate cybersecurity measures;
- encourage manufacturers to incorporate security by design throughout the digital product life cycle; and
- supplement existing cybersecurity regulations, including the NIS2 and DORA.

## 5. Security Certification for ICT Products, Services and Processes

### 5.1 Key Cybersecurity Certification Legislation

#### The Cybersecurity Act

The Cybersecurity Act entered into force on 27 June 2019. The primary goal of the Cybersecurity Act is to enhance protection against cybersecurity threats across the EU. The Cybersecurity Act also enables manufacturers and service providers to use one mutually recognised certificate throughout the EU.

#### Main Elements

The regulation has two main functions and purposes:

- to give the EU Agency for Network and Information Security a permanent mandate, more resources and new tasks; and
- to create a framework for certifying cybersecurity products and services; this framework sets up a system to govern the issuance of European cybersecurity certificates and declarations of conformity with security standards for ICT products, services, and processes, and the purpose of the certification is to guarantee that users are provided with adequate information regarding the relevant cybersecurity features.

#### National Cybersecurity Certification Authority

In Sweden, the Swedish Defence Materiel Administration acts as the national cybersecurity certification authority. It is the cybersecurity and certification department at the Swedish Defence Materiel Administration that is responsible for matters related to cybersecurity certification, supervision, collaboration, and external monitoring. The department consists of the Swedish Certification Body for IT Security and the Swedish Cyber Security Certification Authority.

Furthermore, the Swedish Defence Materiel Administration is tasked with overseeing and coordinating certification activities at the national level and collaborating with EU entities such as the EU Agency for Network and Information Security and the European Commission. It also serves as Sweden's representative in the European Cybersecurity Certification Group.

Additionally, the Swedish Defence Materiel Administration is responsible for notifying the EU about accredited bodies and those authorised under the Cybersecurity Act.

## 6. Cybersecurity in Other Regulations

### 6.1 Cybersecurity and Data Protection

#### GDPR and Swedish Supplementation

The GDPR aims to protect natural persons when processing personal data. In Sweden, the GDPR is supplemented by the Data Protection Act, which contains supplementary provisions to the GDPR.

### Controller Responsibilities and Data Processing Agreements

A legal entity that determines the purposes and means of processing personal data is a controller under the GDPR. While a controller can appoint a processor to process data on its behalf, the ultimate responsibility for compliance remains with the controller. To ensure the processor adheres to GDPR requirements, the parties must enter into a data processing agreement that governs the processing activities and outlines both parties' obligations and rights.

### Protective Measures and Data Subject's Rights

The GDPR requires controllers to implement appropriate technical and organisational measures to protect the processed personal data from unauthorised access. The appropriate measures should be determined based on the risk of the processing. This may include:

- pseudonymisation and encryption of personal data;
- ensuring ongoing confidentiality, integrity, availability, and resilience;
- ensuring data restoration; and
- regularly testing, assessing, and evaluating measures.

The controller must also inform data subjects about the processing of their personal data and of their rights. The data subject's rights include:

- right to access personal data and information;
- right to rectification;
- right to erasure;
- right to restriction of processing;
- right to data portability; and
- right to object.

### Data Breach

Entities processing personal data must adhere to the GDPR's specific provisions regarding personal data breaches. A personal data breach involves a security incident resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

If a breach risks individuals' rights and freedoms, the controller must notify the Swedish Authority for Privacy Protection within 72 hours of awareness.

The notification shall at least include a description of:

- the nature of the breach;
- the likely consequences of the breach;
- the measures taken or proposed to mitigate the consequences of the breach; and
- contact information for further inquiries.

If a breach likely poses a high risk to individuals' rights and freedoms, the data subject should generally be informed. All breaches must be documented by the controller, regardless of risk level.

However, it should be noted that the Data Protection Act stipulates that if an incident that constitutes a personal data breach is to be notified under the Protective Security Act, the notification and information obligations under Articles 33 and 34 of the GDPR shall not be applicable.

## 6.2 Cybersecurity and AI

The Swedish government has launched an inquiry to evaluate the need for national adjustments in response to the AI Act. The inquiry will recommend necessary legal changes and

measures for transparency and oversight, with the final report due by 30 September 2025.

The AI Act, effective from 1 August 2024, establishes a unified framework for AI development and use within the EU. It categorises AI systems based on risk levels, imposing stricter requirements on high-risk applications, such as those in critical infrastructure, healthcare, and law enforcement. For Sweden, this means adapting national regulations to comply with EU standards, ensuring AI systems are human-centred, reliable, and aligned with fundamental rights. This includes mechanisms for oversight and enforcement to maintain high protection levels for health, safety, and fundamental rights.

The AI Act imposes obligations primarily on AI providers, developers, and commercial users to ensure compliance with its standards. Such obligations include:

- classifying AI systems by risk levels, with stricter requirements for high-risk applications;
- ensuring AI systems are transparent and understandable to users;
- implementing mechanisms for oversight and accountability;
- meeting safety standards; and
- ensuring high-quality data management and protection.

## 6.3 Cybersecurity in the Healthcare Sector

### The Patient Data Act and the Patient Data Regulation

The healthcare sector must systematically address the security of healthcare information management. Cybersecurity in healthcare focuses on safeguarding electronic information and assets against unauthorised access, use, and disclosure.

The Patient Data Act contains explicit provisions to prevent unauthorised dissemination by electronic means of data relating to patients undergoing treatment. It contains the provisions specifically needed for the processing of patient data by healthcare providers in relation to other personal data processing. Otherwise, the provisions of the GDPR apply to the processing of patient data and other personal data by healthcare providers. The Patient Data Act governs several aspects, including:

- the ability of healthcare personnel involved in a patient's care to access necessary medical records, even if those records were created by a different healthcare organisation;
- the regulations determining which individuals are permitted to access patient data as part of their duties within the healthcare system; and
- the patient's right to restrict access to information in their medical records within an electronic records system.

# Trends and Developments

**Contributed by:**
Anders Bergsten and Victoria Nordenberg
**Mannheimer Swartling**

**Mannheimer Swartling** is the largest law firm in the Nordics and is a leading adviser in the premium segment for business law in Sweden. Its full-service practice is unique for Sweden in that the lawyers have a high degree of specialisation. The firm can therefore cover all the specialist advice needs of its clients – of any size or complexity – in-house. The corporate commercial team consists of 75 lawyers based in Stockholm, Gothenburg and Malmö. The team regularly acts on large IT procurements and outsourcings where complex cybersecurity issues arise. Cybersecurity matters within digitalisation projects, online currencies and collaboration agreements are also frequently handled by the team. Another strength is data protection mandates ranging from GDPR compliance to data breaches. Clients also benefit from the team's close collaboration with the M&A department to assist with technology-related set-ups. Clients from the healthcare, automotive and technology sectors mandate Mannheimer Swartling.

## Authors

**Anders Bergsten** is a member of Mannheimer Swartling's corporate, tech and IP practice group, and is based in Stockholm. He advises clients on a wide range of national and international commercial matters, focused on the IT and technology area. Anders' practice consists mainly of advising on complex delivery, outsourcing and procurement projects, together with advising on cybersecurity, protective security, digital compliance and personal data matters. Anders joined the firm in 2006 and is a member of the Swedish Bar Association. He has an LLM degree from the University of Uppsala and has studied law at the University of Sydney.

**Victoria Nordenberg** is a member of Mannheimer Swartling's corporate, tech and IP practice group. She advises Swedish and international clients across a wide range of industries, with a particular focus on societal functions and critical infrastructure. Victoria has extensive experience in drafting and negotiating IT contracts, outsourcing agreements and other complex commercial agreements. In addition, Victoria has significant experience working with cybersecurity and digital communications regulation. Victoria joined the firm in 2016 and is a member of the Swedish Bar Association. She holds an LLM degree from the University of Uppsala.

Mannheimer Swartling
Advokatbyrå AB

Norrlandsgatan 21
111 43
Stockholm
Sweden

Tel: +46 859 506 000
Fax: +46 859 506 001
Email: felicity.trocme@msa.se
Web: www.mannheimerswartling.se


## Digitalisation and Cyber-Attacks

Sweden is a leading nation in the research and development of new technologies, with digitalisation at the heart of its progress. However, the deteriorating global security landscape has increased the risk of cyber-attacks, which makes highly digitised countries extra vulnerable. Like in many other countries, both public and private entities in Sweden are repeatedly targeted by cyber-attacks from foreign powers (either state actors or threat actors acting with the tacit acceptance from host nations). Consequently, the ability to effectively manage these cyber threats is crucial for Swedish organisations, leading to an increased need for robust protection against such attacks. This has led to an increased need for robust protection against cyber-attacks.

In Sweden, cyber threats manifest themselves in various forms, including intelligence threats from foreign powers and criminal activities targeting companies. These threats often involve tactics such as phishing, password attacks, malware and attacks on mobile devices and email systems. As cyber-attacks continue to evolve and become more sophisticated, it is imperative for every organisation to regularly ensure that its defences remain robust and effective. Protection against cyber-attacks is particularly important for organisations that provide essential societal functions and manage critical IT systems. The direct and indirect costs of cyber-attacks on such operations are estimated to be in the billions of Swedish kronor yearly.

It should be noted that the Swedish regulatory environment concerning cybersecurity has not entirely kept pace with the swift deterioration in the global security landscape, together with the adoption of many EU initiatives. To a certain extent, this has led to a somewhat fragmentized regulatory picture – eg, in relation to supervisory authorities and notification obligations in case of incidents caused by cyber-attacks.

## Extended Applicability

In the past, the legal obligations to meet certain cybersecurity requirements have been directed at public authorities, whereas now the regulatory framework will require substantial security measures from a much broader group of organisations, including private companies. In 2019, the applicability of the Protective Secu-

rity Act (*Säkerhetsskyddslagen (2018:585)*) was extended from public entities to all types of entities whose operations are of importance to Sweden's security. Similarly, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2) and Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER), which will be transposed into Swedish law later this year, will apply to both private and public entities and will require extensive cybersecurity measures to be taken.

### Increased Sanctions

With the increased focus on cybersecurity and security measures, one of the tools that legislators are using to enforce the importance of cybersecurity is to increase sanctions. This tool has been used in relation to both NIS2 and CER, where an operator that fails to comply with NIS2 or CER can be fined up to the higher of 2% of its total worldwide annual turnover in the preceding financial year or EUR10,000,000.

In order to create a common basis and applicability, the Swedish government's official report on the transposition of CER into Swedish law, SOU 2024:64, proposes that a failure to comply with the Protective Security Act is prohibited in a similar manner, and the proposal is to increase the sanction to the greater of SEK120,000,000 (approximately EUR12,000,000) or 2% of the operator's total annual global turnover from the previous financial year.

### National Cybersecurity Centre

Due to the increased focus on cybersecurity in Sweden, the Swedish Armed Forces, the National Defence Radio Establishment, the Swedish Civil Contingencies Agency and the Swedish Security Service, launched the National Cybersecurity Centre in December 2020 with the mission to strengthen Sweden's overall ability to prevent, detect and manage cyber threats. From November 2024, the National Cybersecurity Centre is part of the National Defence Radio Establishment, which coincides with the government raising its ambitions for the centre.

The NCSC is responsible for strengthening Sweden's cybersecurity and is now expected to expand its responsibilities. These new responsibilities include acting as a central body to co-ordinate and support national cybersecurity efforts. This involves monitoring and analysing cyber threats, providing advice and support to both public and private organisations, and promoting information sharing and collaboration among various cybersecurity stakeholders. The NCSC will also improve the ability to analyse and assess cyberthreats, vulnerabilities and other risks regarding information- and cybersecurity.

### Common Level of Security Measures Within the Union

Sweden is not the only EU member state that has an increased focus on cybersecurity. The EU is adopting several robust regulatory frameworks that require comprehensive security measures, some of which are expected to be transposed to binding Swedish law during 2025 and some of which Swedish entities should monitor during the year.

#### *NIS2*

The NIS2 directive was adopted by the EU in December 2022, repealing and replacing Direc-

tive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

The directive aims to harmonise and strengthen cybersecurity in the Union. It sets out requirements for technical, operational and organisational measures to manage risks that threaten the security of network and information systems. These measures should include risk analysis, business continuity measures, supply chain security measures and personnel security measures. The measures should be based on an overall risk perspective and risk analysis and be proportionate to the risk. They should be evaluated and include specific elements, including supply chain security. Supply chain security covers security aspects relating to the links between each operator and its direct suppliers or service providers. This means that each operator must take risk management measures in relation to its suppliers and is therefore responsible for its direct suppliers.

In addition, NIS2 requires policies and procedures to assess the effectiveness of cybersecurity risk management measures and to address any deficiencies. NIS2 also requires senior management to monitor the implementation of risk management measures.

In the event of an incident that has a significant impact on an entity's ability to provide its services, the directive requires the entity to notify the competent authority of the incident. If deemed appropriate, service recipients should also be informed of the incident. An incident is considered significant if it causes, or has the potential to cause, severe operational disruption to services, results in financial losses for the entity, or has, or could have, an impact on other natural or legal persons by causing considerable damage.

As proposed in the Swedish government's official report 2024:18, NIS2 will be implemented in Sweden through the Swedish Cybersecurity Act (*cybersäkerhetslagen*) (the "Swedish Cybersecurity Act") and the Swedish Cybersecurity Regulation (*förordning om cybersäkerhet*), which will replace the current Act on Information Security for Critical and Digital Services *(lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*) and the Regulation on Information Security for Critical and Digital Services (*förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster*). The government has not yet proposed a bill, but it is expected to do so in the spring of 2025. As NIS2 should have been implemented in the member states by 18 October 2024, and Sweden is already behind, it is expected that the time between the bill being passed and it coming into force will be short.

Once the Act comes into force, clarifying regulations will be issued by the designated authorities and only then will the detailed requirements for affected entities be clear. It has not yet been decided which authorities will be responsible for the regulations.

### *CER*

To enhance the EU's resilience in critical infrastructure, the EU has adopted a directive aimed at ensuring that essential services can effectively prevent, withstand, and manage disruptions or interruptions in their operations. The CER is proposed to be transposed in Sweden through the Critical Operators Resilience Act (*lag om motståndskraft hos kritiska verksamhetsutövar*e) and the Critical Operators Resilience Regulation (*förordning om motståndskraft hos kritiska*

*verksamhetsutövare*) as described in the Swedish government's official report 2024:64. The government has not yet proposed a bill, but it is expected to do so in the spring of 2025.

Once transposed, there will be an increase in cybersecurity requirements, and other related measures, for critical entities in Sweden as the Directive replaces the previous Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, which was more limited in scope.

The CER applies to critical entities providing services in the following sectors:

- energy;
- transport;
- banking;
- financial market infrastructure;
- health;
- drinking water;
- waste water;
- digital infrastructure;
- public administration;
- space; and
- production, processing and distribution of food.

Each EU member state must list all essential services within each sector and conduct a risk assessment based on the list. Following the risk assessment, each EU member state will determine which entities are considered critical entities within each sector.

For an entity to be considered a critical entity in Sweden, the following is required:

- the entity must provide an essential service;
- the entity must operate in Sweden and have its critical infrastructure in Sweden; and
- an incident affecting the entity must significantly disrupt its ability to deliver its essential services or impact other essential services within the sectors covered by the law.

Once identified, a critical entity must perform a critical entity risk assessment. The assessment aims to identify any relevant risks associated with the delivery of the essential service and consider interdependencies with other sectors covered by the law. Based on the risk assessment, the critical entities must implement appropriate and proportionate technical, security and organisational measures to ensure resilience. These measures include preventing incidents, ensuring physical protection, mitigating the consequences of incidents, and recovering from them. Further, a critical entity must also report incidents that have or may have significant disruption to the competent authority without undue delay.

### *CRA Act*

The Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (CRA) was adopted in the EU on 10 December 2024 and will enter into full force on 11 December 2027. However, certain parts of the CRA will enter into force during 2026.

The objective of the CRA is to strengthen EU cybersecurity and ensure cyber resilience by establishing a legal framework for essential cybersecurity requirements for digital elements in the EU. This will be implemented through restrictions on the development of secure products with digital elements to ensure that prod-

ucts in the EU are less vulnerable and more secure throughout their life cycle. The CRA also aims to improve transparency regarding the support period for products.

The CRA does not require transposition into Swedish law and will be directly applicable in Sweden when it enters into force, but additional provisions and adjustments to existing provisions may be necessary. These possible provisional additions and adjustments are currently being examined.

### *AI Act*

As Europe becomes more digitised, the use of artificial intelligence is becoming more widespread. As a result, the EU has adopted Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 ("AI Act").

The AI Act entered into force on 1 August 2024 and will be fully applicable two years later, on 2 August 2026, with certain exceptions including prohibitions and obligations relating to AI competencies that entered into force on 2 February 2025 and governance rules and obligations for general-purpose AI models that will apply from 2 August 2025.

The AI Act aims to create a coherent framework for the development and use of AI systems across the Union. It promotes human-centred and trustworthy AI while ensuring a high level of protection for health, safety and fundamental rights. The AI Act prohibits certain uses of AI, while other uses are restricted depending on the risk level of the AI application. If an AI system is classified as high risk, it must have an appropriate level of accuracy, robustness and cybersecurity.

The AI Act constitutes Swedish law but requires complementary national provisions. These complementary provisions are currently under review and are expected to include proposed provisions for the following:

- the establishment of a system for market surveillance, market monitoring, compliance management; and
- other necessary national adaptations resulting from the AI Act.

## CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com