ecgi

# The Regulation of Data Privacy and Cybersecurity

Law Working Paper N° 853/2025
July 2025

Jasmin Gider
Tilburg University

Luc Renneboog
Tilburg University, CentER and ECGI

Tal Strauss
Tilburg University and European Central Bank

ECGI Working Paper Series in Law

# The Regulation of Data Privacy and Cybersecurity

Working Paper N° 853/2025

July 2025

Jasmin Gider
Luc Renneboog
Tal Strauss

## Abstract

Data privacy protection is stronger in the European Union (EU) compared to the U.S.: EU organisations must generally obtain a valid legal basis, often explicit consent, before collecting, storing or processing personal data from individuals who have the right to withdraw their consent at any time; conversely, in the U.S., privacy assurances in the contexts of law enforcement and national security at the federal level are industry-specific. The European General Data Protection Regulation (GDPR) has a wide scope, covering areas such as data protection impact assessments, data breach notification, and privacy by design. In the U.S., data privacy protection and disclosure of breaches are delegated to the states such that there is no unified framework with definitions of a (material) data breach, reporting thresholds, enforcement responsibilities, penalties for violations, and application scope. Yet, mandatory disclosure regulation of data breaches and privacy violations are still insufficient in both Europe and the U.S. In relation to regulations in the realm of fighting cybercrime through the implementation of minimum cybersecurity levels, this paper demonstrates how complex, heterogenous, and incomplete the regulatory landscape is. Remarkably, there is no encompassing up-to-date federal law regulating cybersecurity in the U.S. as this regulation was delegated to the individual states who are responsible for standard setting and compliance. Furthermore, cybersecurity regulation has been developed for specific industries and critical infrastructure. This has resulted in a proliferation of enforcement agencies with heterogeneous standards, reporting requirements, and penalties. While publicly-traded companies must disclose material cyber events according to securities regulation, these ad-hoc disclosure requirements are even less stringent in Europe. While the EU and the U.S. agree on the importance of certification and baseline cybersecurity requirements, they have different approaches. EU member states require all organisations to follow the Directive on security of Network and Information Systems (NIS Directive) for the best safeguards, while the adoption of the National Institute of Standards and Technology Cybersecurity (NIST) Framework for cybersecurity crisis management is voluntary in the U.S.

---

Keywords: Data privacy, Cybersecurity, Data protection, Data breach, Cyber attack, Cyber Incident, GDPR

JEL Classifications: G18, L51, K24, K23, F55

Jasmin Gider
Associate Professor
Tilburg University
PO Box 90163
5000 LE Tilburg, Netherlands
e-mail: J.Gider@uvt.nl

Luc Renneboog*
Professor of Corporate Finance
Tilburg University, School of Economics and Management, Department of Finance
Warandelaan 2
5037 AB Tilburg, The Netherlands
phone: +31 134 668 210
e-mail: luc.renneboog@tilburguniversity.edu

Tal Strauss
Researcher
Tilburg University
PO Box 90163
5000 LE Tilburg, Netherlands
e-mail: T.Strauss@tilburguniversity.edu

*Corresponding Author

# The Regulation of Data Privacy and Cybersecurity

**Jasmin Gider**[a]
*Tilburg University*
**Luc Renneboog**[b]
*Tilburg University and ECGI*
**Tal Strauss**[c]
*Tilburg University and European Central Bank*

**Abstract:**

Data privacy protection is stronger in the European Union (EU) compared to the U.S.: EU organisations must generally obtain a valid legal basis, often explicit consent, before collecting, storing or processing personal data from individuals who have the right to withdraw their consent at any time; conversely, in the U.S., privacy assurances in the contexts of law enforcement and national security at the federal level are industry-specific. The European General Data Protection Regulation (GDPR) has a wide scope, covering areas such as data protection impact assessments, data breach notification, and privacy by design. In the U.S., data privacy protection and disclosure of breaches are delegated to the states such that there is no unified framework with definitions of a (material) data breach, reporting thresholds, enforcement responsibilities, penalties for violations, and application scope. Yet, mandatory disclosure regulation of data breaches and privacy violations are still insufficient in both Europe and the U.S.

In relation to regulations in the realm of fighting cybercrime through the implementation of minimum cybersecurity levels, this paper demonstrates how complex, heterogenous, and incomplete the regulatory landscape is. Remarkably, there is no encompassing up-to-date federal law regulating cybersecurity in the U.S. as this regulation was delegated to the individual states who are responsible for standard setting and compliance. Furthermore, cybersecurity regulation has been developed for specific industries and critical infrastructure. This has resulted in a proliferation of enforcement agencies with heterogeneous standards, reporting requirements, and penalties. While publicly-traded companies must disclose material cyber events according to securities regulation, these ad-hoc disclosure requirements are even less stringent in Europe.

While the EU and the U.S. agree on the importance of certification and baseline cybersecurity requirements, they have different approaches. EU member states require all organisations to follow the Directive on security of Network and Information Systems (NIS Directive) for the best safeguards, while the adoption of the National Institute of Standards and Technology Cybersecurity (NIST) Framework for cybersecurity crisis management is voluntary in the U.S.

a. Jasmin Gider, Dpt of Finance, Tilburg University, POBox 90153, 5000 LE Tilburg University, the Netherlands. Email: J.Gider@uvt.nl
b. Luc Renneboog, Dpt of Finance, Tilburg University, POBox 90153, 5000 LE Tilburg University, the Netherlands. Email: Luc.Renneboog@uvt.nl
c. Tal Strauss, Dpt of Finance, Tilburg University, POBox 90153, 5000 LE Tilburg University, the Netherlands, and The European Central Bank, Sonnemannstraße 20, 60314 Frankfurt am Main. Email: Tal.Strauss@ecb.europa.eu

Keywords: **Data privacy; Cybersecurity; Data protection; Data breach; Cyber attack; Cyber Incident; GDPR**

JEL codes: **G18; L51; K24; K23 and F55**

Note: The views expressed in each article are those of the authors and do not necessarily represent the views of the European Central Bank.

# The Regulation of Data Privacy and Cybersecurity

## 1. Introduction

The growth of cyberattacks and data breaches poses an increasingly alarming threat to public and private corporations, organisations, and government agencies. The costs are rising to an extent that cyber-related risks may become uninsurable. The cybercrime costs - costs of damaged and destroyed data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack business disruption, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm – are predicted to reach USD 10.5 trillion in 2025, more than tripling from USD 3 trillion in 2015 (Cybersecurity Ventures 2025). With a predicted annual growth of 2.5%, the total cybercrime costs will amount to USD 12.2 trillion annually.

Our own analysis on data breaches and cyber incidents at listed U.S. companies over the period from 2005 to 2023 confirms the massive increase in reported events: from about 59 incidents in 2005 to 1964 already in 2013.[1] Figure 1 also partitions the total number of cyber incidents in the following categories (in order of frequency of occurrence): malicious data breach (about 56% of the incidents); Unintentional disclosure (15%); Stolen data (10%); Phishing/spoofing (8%); Network disruption (5%); IT errors (4%); Identity theft (0.1%); and other (0.01%). Data breaches encompass the exposure of corporate and private information through system compromise, negligence, and misconduct (e.g., cyber-incidents resulting in encrypted IT systems) and result from attacks on e-commerce websites leading to the theft of personal information and corporate secrets, such as patents, R&D, or vaccine development from healthcare organisations. Physical breaches include instances of stolen or lost laptops, U.S.Bs, and other physical devices. These breaches often result in the compromise of confidential company information, social security numbers, account data, and other personal information.

The known and reported number of exposed records in 16,409 incidents in listed U.S. firms over the period 2005-2023 amount to approximately 5 billion records. The number of records exposed is given in Figure 2 with most records stolen at cyber breaches initiated by an external (hostile) nation state and criminal organisation. Breaches attributed to unknown external actors had a median exposure of about 150 records. In contrast, incidents caused by internal organisational actors and employees had lower median exposures of fewer than 10 records. Criminal actors were associated with the most severe typical impact, with a median loss of about 3,000 records, while breaches involving related parties had a median exposure of around 40 records. Although most incidents were limited in scale, often involving fewer than a few hundred records, the data exhibit substantial right-skewness. At the 99th percentile,

[1] The data comprise a sample of the database of Zywave.

incidents in several perpetrator categories involved hundreds of thousands to over 20 million records, indicating that a small number of extreme cases account for a disproportionately large share of total records exposed.

These numbers serve as a lower bound estimate because not all breaches are discovered by the firms themselves and firms are likely to underreport, given the patchy mandatory disclosure framework and firms' preference to protect their reputation. Some attacks have a cascading effect, such as the 2008 hacking incident at Heartland Payment Systems, which resulted in the theft of credit card information from over 1.3 million accounts and impacted over 100 financial institutions. In most cases, the perpetrator cannot be identified, and one can thus only suspect the identify or location of the offender. For instance, in the majority of cases, major data losses are suspected to originate primarily from hackers associated with or acting on behalf of foreign nation states, whereas only a small fraction are attributed to identified criminal organisations or individual offenders.

*Nation-state* cyber incidents, which are currently on the rise due to an increase in geopolitical tensions, can result in significant losses of records, affecting sensitive information such as personal data, financial information, trade secrets, and confidential government documents. These types of attacks are often well-coordinated and executed with advanced tools and techniques, making them particularly difficult to detect and defend against. Some of the most notable examples include the SolarWinds supply chain attack, the Equifax data breach, and the breach of the Office of Personnel Management (OPM[2]) in the U.S. In each of these incidents, sensitive information was stolen and potentially used for malicious purposes, such as identity theft or espionage. The impact of nation-state cyber incidents on records loss can be significant, both for the individuals and organisations whose data is stolen, as well as for the nation as a whole. In addition to the immediate loss of sensitive information, nation-state cyber incidents can also have long-term consequences, such as damage to a country's reputation, loss of trust in government and financial institutions, erosion of trust in the democratic system following manipulation of elections, and economic harm to corporations. Cyber incidents perpetrated by criminal organisations vary in severity, ranging from unauthorized access to sensitive data, to ransomware attacks that encrypt crucial records and demand payment in exchange for their release. In many cases, criminal organisations target businesses and institutions that store valuable personal and financial information, such as credit card numbers, social security numbers, and medical records. These types of data are highly sought after by criminal organisations for use in identity theft, fraud, and other illegal activities. When a cyber incident occurs, organisations may lose access to their records, or the records may be stolen and sold on the black market (on the dark web). In some cases, records may be permanently lost, causing significant financial and reputational damage to the affected organisations and their clients. Figure 2 shows that a substantial share of data breaches originates from actors within or closely connected to the targeted organisation, including internal departments, employees, and related parties, often due to negligence or weak controls. Only a negligible portion of breaches is linked to hacktivist activity, while a modest share results from unintentional or deliberate

[2] The glossary with abbreviations is given in Appendix 1.

information leaks by the firm's own employees, consultants, or vendors. Cyber incidents that result in the loss of records by an internal trusted third party can have serious consequences for organisations, often resulting in the loss of a substantial volume of records. This highlights the importance of having proper access controls and security protocols in place to prevent unauthorized access to sensitive data. The loss of records by an internal trusted third party can occur due to a variety of reasons, including negligence that facilitates hacking, employee error, or malicious insider activity. Internal trusted third parties typically have access to sensitive data, making them an attractive target for cybercriminals. For example, an internal trusted third party may be the target of a phishing attack that resulting in data theft. Similarly, an employee of the trusted third party may accidentally delete critical records, or a malicious insider may intentionally compromise the data. A cyber incident involving a *hacktivist* group can also result in a significant loss of records. Hacktivist groups are motivated by political or social causes and often target organisations that they believe are opposing their beliefs. In a cyber incident involving a hacktivist, sensitive data such as customer records, financial information, and trade secrets may be stolen and potentially leaked. This can result in a significant loss of trust among customers, damage to the company's reputation, and financial losses from lawsuits and the cost of recovering from the attack.

The damages caused by data breaches and cyberattacks can be substantial. Figure 3 provides more details on over 12,000 incidents with identified attack vectors. On average, incidents involving system vulnerabilities cause the highest financial losses, exceeding USD 140 million per breach. Misconfiguration issues result in average damages of around USD 90 million, while malware and access or privilege misuse lead to costs of roughly USD 70 million each. Ransomware attacks, although slightly less costly on average, still impose average damages of around USD 20 million. *System vulnerabilities* are weaknesses in software or hardware systems that can be exploited by attackers to gain unauthorized access, steal sensitive information, or disrupt operations. Direct financial damage can include costs associated with repairing or replacing damaged systems, as well as the cost of notifying customers and the loss of business as a result of damage to the company's reputation. Indirect financial damage can be even more significant, as attackers may use system vulnerabilities to gain access to financial records or trade secrets. This information can then be used to steal money, disrupt operations, or damage the organisation's reputation. Additionally, system vulnerabilities can also lead to downtime, which can result in lost productivity and revenues. *Access or privilege misuse* refers to the unauthorized use of systems, applications, or data by individuals who have been granted access privileges. This type of cyberattack can cause significant financial damage to organisations. Direct financial damage can include the cost of repairing or replacing damaged systems and the cost of any data breaches, such as the cost of notifying customers and the loss of business as a result of damage to the company's reputation. In the case of *ransomware*, attackers typically encrypt the victim's data and demand a ransom payment in exchange for the decryption key. Failure to pay the ransom can result in the permanent loss of data, which can have a significant impact on an organisation's operations and reputation. Furthermore, attackers may misuse access privilege to steal sensitive information such as financial records or trade secrets. *Misconfiguration* refers to the incorrect setting of system parameters,

which can leave systems vulnerable to attack. This type of incidents can be caused by human error, poor documentation, or simply a lack of understanding of how to properly configure systems. *Malware* can cause financial damage in a variety of ways, such as stealing sensitive information, disrupting operations, and spreading to other systems, leading to widespread damage.

Malware can cause financial damage in a variety of ways, such as stealing sensitive information, disrupting operations, and spreading to other systems, leading to extensive damage.

[Insert Figures 1-3 about here]

The rising number of cyber incidents as well as their increasing severity and costs to a wide range of stakeholders have led to the emergence of a plethora of rules and regulations to fight cyber threats and mitigate the harm and potential externalities. There is also older, existing regulation that has not been designed to address cyber problems as it predates the internet, while it still applies to data breaches and cyber risk. This paper provides a structured overview of the existing and planned regulations in place in both the U.S. and in the European Union, and intends to navigate the highly fragmented regulatory aspects that govern cyber risk. Moreover, we analyze and compare the coverage and approaches of both jurisdictions, clarifying their emphasis and potential gaps.

The overarching objective of cybersecurity regulation (against cyberattacks and data privacy breaches) is to protect:

(a.) private information of individuals which includes data on their health, identity, employment, and finances,

(b.) proprietary corporate data about technology, products, employees, investors, customers, and suppliers,

(c.) corporations' operational ability as going concerns,

(d.) the security of nation states (infrastructure, energy, administration, etc.).

We distinguish between two types of regulation:

1. Mandatory protection levels and minimum technical standards.
2. Data breach notification and fines.

The security levels and minimum technical standards imposed by regulation are set to provide a minimum expected level of protection. Some of these regulations are industry-specific, such as the regulation targeted at the protection of critical infrastructure. An example is the European Cybersecurity Act (EU 2019/881), which seeks to ensure that firms and organisations selling, offering, or protecting IT products, services, infrastructure, and processes take sufficient cybersecurity measures. Another example is the Network and Information Systems (NIS) Directive (EU 2016/1148), which requires countries to protect their vital services and digital service providers. The data breach notification

regulations give individuals affected by data breaches the right to be notified of such incidents. Further, certain regulations go beyond the mere reporting of breachers to the affected persons and organisations, but also mandate disclosure of these events to other stakeholders, such as investors, or the general public.

Mandatory disclosure of data breaches enables individuals (e.g., customers, employees, patients), investors (e.g., shareholders, bondholders), and firms (e.g., suppliers and customers) to hold firms liable for negligence. Breach laws also introduce penalties for companies and organisations in case of breaches, effectively forcing them to internalize potential externalities that cyberattacks can create for affected stakeholders. Examples include Europe's General Data Protection Regulation (GDPR; EU 2016/679) or the proposed Consumer Privacy Protection Act of 2017 (CPPA – never enacted) in the U.S., which aims to safeguard the privacy and security of sensitive personal data, prevent, and reduce identity theft, and notify people when their personal data are compromised. These laws also improve transnational cooperation regarding law enforcement and require the activation of safeguards against security lapses, unauthorized access, and misuse of personal data. We provide a detailed summary of cyber-related regulations across the U.S. and Europe in Appendix 2, which we discuss in the following subsections.

## 2. European Union Regulation

In October 1995, the European Commission (EC) enacted the Data Protection Directive (95/46/EC) to supervise the processing of personal data and the conditions of free movement of such data. It was the first concerted EU-wide regulation that encompassed data treatment and acknowledged its importance. The Directive defined the scope of personal data, extended to the processing, storing, and sharing of data, and illuminated the need for 'data subject consent'. The Directive laid the foundations for safeguarding natural individuals' basic freedoms and rights, including the right to privacy, when personal data are processed (European Parliament, 1995). National authorities were required to incorporate the Directive in national regulation within four years, which was achieved by all the member states. Since then, the EC has further introduced several data protection acts and acknowledged the significance and financial worth of data.

The Data Protection Directive has led to a dual strategy, focused on data breach notification and fines, and on mandatory protection levels and minimum technical standards.

### 2.1 The General Data Protection Regulation (GDPR)

#### *2.1.1 Guiding Privacy Principles*

The Data Protection Directive was superseded by the General Data Protection Regulation (EU 2016/679) that came into effect on May 24, 2016 and applicable since May 25, 2018. The GDPR, which comprises 11 chapters and 91 articles, is a set of regulations that govern how individuals are protected

when their data are processed by hand or automatically, and enhances the rights of individuals to control their personal data. The regulation applies to businesses and organisations with headquarters in the EU as well as businesses and organisations located outside the EU that process personal data of EU citizens to deliver products or services or keep tabs on their behavior there (European Parliament & Council, 2016); Cole & Schmitz, 2019; Rustad and Koenig, 2019).[3]

The GDPR directly applies to all member states, without the need for national transposition.[4] In terms of reporting requirements, all EU member states are required by the GDPR to notify the European Commission (EC) of the provisions in national data privacy regulations regarding data protection authorities, penalties, and balancing the right to privacy with the freedoms of expression and information (Boehm, 2015). As such, the following provisions should also be reported to the EC if an EU member state has national data protection laws on the processing of personal data for employment purposes, confidentiality obligations, restrictions on the transfer of certain categories of data for vital public interests, and other legal remedies in place of administrative fines (European Commission, 2022a).

GDPR's guiding principles[5] have a fundamental impact on a large portion of the current IT architecture and procedures and can be condensed into three key issues for enterprise IT: (i) data protection and integrity, (ii) risk mitigation, and (iii) increase in control over and visibility of data (Sekaran, 2022). GDPR has led to the following major changes: the requirement of explicit and affirmative consent before the processing of personal data, the overall greater transparency in relation to data processing, data protection by design or default, mandatory data breach notification, and the principle of a one-stop-shop[6] with one lead authority and cooperation procedures. In addition, the regulation introduces additional rights that are advantageous to the data subjects: the right to data portability[7], the right to be forgotten, and extended access rights to one's own data (Wood, 2018; Cole et al., 2020).

### *2.1.2 Enforcement Agencies*

The GDPR is enforced by the individual data protection agencies (DPAs) from the 27 EU member states. These DPAs investigate complaints, offer guidance on data privacy concerns, and identify instances when the GDPR has been violated. DPAs are independent public agencies with the capacity

[3] According to the GDPR, the definition of personal data is any data that relates to a person who can be "used to directly or indirectly identify that person." Names, ID numbers, phone numbers, and email addresses are obvious examples of this, but it can also include IP addresses, browser cookies, or delicate personal information like gender, religious preferences, or political affiliation.

[4] This means that the EU regulation is directly applicable in the member states without the need for each member state to enact its own legislation or take other implementation measures.

[5] The GDPR core principles are laid out in Article 5 (EU, 2022) and are: Lawfulness, fairness, and transparency; Purpose limitation; Data minimization; Accuracy; Storage limitation; Integrity and confidentiality; and Accountability.

[6] This means that to comply with the GDPR, organisations need to cooperate primarily with the supervisory authority located in the same member state as its principal establishment (often the firm's EU headquarters).

[7] This feature refers to the right of individuals to receive a copy of their personal data in a commonly used and machine-readable format.

to investigate and correct violations of the data protection regulation. They offer knowledgeable counsel on data protection matters and address grievances brought up regarding contraventions of the GDPR and pertinent national laws. All DPAs collaborate at the European level in the European Data Protection Board (EDPB), which is headed by the European Data Protection Supervisor (EDPS). The EDPB seeks to enforce the GDPR uniformly throughout the EU and oversees the advice given to member states on complex cyber subjects or the proper execution of the legislation. When the EC examines privacy and data protection laws or issues, the EDPB formulates opinions (yet the EDPB does not enforce data protection legislation).

Generally, in cases where the GDPR applies, national data protection rules do not apply because the GDPR supersedes national law, with some exception of the gathering and processing of employee data or the designation of a data protection officer, issues of national security, and crime prevention and investigation, which are not fully governed by GDPR.[8] As a consequence of the above exceptions to the universal validity of GDPR to all member states, there may still be some differences across states, which relate to variances in countries' corporate liability rules, the interpretation of data breach evidence, and the procedures on how to address violations.[9] It is worthwhile pointing out that the GDPR is no longer applicable in the UK since Brexit. Entities inside the UK must comply with the Data Protection Act 2018, which is the UK's Act on the lawful processing of personal data. The GDPR only applies to a UK entity if it operates in the European Economic Area (EEA) by offering services and goods or monitors the behaviour of persons within the EEA[10] (Information Commissioner's Office, 2022).

### *2.1.3 The Penalties for GDPR Violations*

GDPR supports consumer privacy rights and mandates the application of data protection standards. The enforcement of data protection laws is handled by member states' data protection agencies rather than a centralized body at the European level. GDPR infractions are subject to two levels of fines, the conditions of which are detailed in Article 83. Infringements on the controller and processor's obligations governed by the monitoring body (The European Data Protection Board or EDPD[11]) or a certification body (e.g., International Association of Privacy Professionals or IAPP), carry first-tier penalties with fines of up to EUR 10 million or up to 2% of the global annual turnover (gross revenue

[8] The GDPR provides specific provisions and exemptions in relation to the processing of employee data, to ensure that the regulation does not unduly burden employers or impede legitimate business activities. For example, the GDPR permits the processing of employee data where necessary for the performance of an employment contract or for compliance with a legal obligation, without requiring the employer to obtain additional consent from the employee.

[9] For example, in 2020, the federal administrative court in Austria overturned a decision to impose a fine on the Austrian post, claiming the Austrian procedural law requires proof that the company violated the GDPR. In contrast, the French Parliament trusts that the "CNIL" (French SA) only needs to portray the fine's motives consistent with Article 83 of the GDPR, without discussing any other criteria, or explaining the fine's calculation.

[10] Refers to the tracking, profiling, or other forms of systematic observation of individuals' behaviour that take place within the EEA. This could include any kind of online tracking or profiling, such as the use of cookies or other digital tracking technologies to collect information about individuals' browsing or purchasing habits.

[11] The EDPB is an independent body of the European Union that is responsible for ensuring consistent application of data protection rules throughout the EU.

of the prior fiscal year), whichever is higher. More egregious violations of the fundamental principles for data processing (including the requirements to ask the consent of the individuals or companies of which the data are used) are called second tier penalties and can be subject to fines of up to EUR 20 million, or up to 4% of the global annual turnover, whichever is higher. These fundamental breaches relate (a) to the rights of the data subjects (including the sending of personal data to a recipient in a third country or an international organisation), any commitments made under Chapter IX[12] in pursuance of member state law, the rules set in the Directive, the failure to grant access to data processing or the holdup of data flows by the supervisory authority, or (b) to granting access in violation of Article 58, (which sets out the powers and duties of the supervisory authorities in enforcing and monitoring the GDPR).

The European enforcement agencies can impose substantial fines for GDPR violations. The largest GDPR fine to date was given by the Luxembourg's National Commission for Data Protection (CNPD) on July 16, 2021, to Amazon for an amount of EUR 746 million. The fine results from a complaint made in May 2018 by 10,000 persons through the French privacy rights organisation La Quadrature du Net. According to this complaint, Amazon used customers' personal information without their permission for targeted adverts. For the same reason, the Irish Data Protection Commission (DPC), Ireland's GDPR supervisory authority, fined Instagram for EUR 405 million on July 28, 2022, making it the second largest GDPR fine.[13] In this case, the two main complaints related to "the public disclosure of email addresses and/or phone numbers of children using the Instagram business account feature and a public-by-default setting for personal Instagram accounts of children".[14]

On 10 July 2023, the European Commission adopted an adequacy decision for the EU–U.S. Data Privacy Framework, establishing that the United States ensures an adequate level of protection for personal data transferred from the EU to U.S. companies participating in the framework. This decision facilitates the free and safe flow of personal data between the EU and the U.S., addressing concerns raised by the European Court of Justice in the Schrems II decision. Key features of the framework include binding safeguards to limit U.S. intelligence agencies' access to EU data to what is necessary and proportionate, the establishment of a two-tier redress mechanism for EU individuals, including the

[12] Chapter IX covers "Provisions relating to specific processing situations", e.g., processing of personal data for scientific, historical, or statistical research purposes.

[13] U.S. data scientist David Stier was the source of the information that initially sparked the investigation in September 2020. Several Concerned Supervisory Authorities (CSAs) objected to the case being sent to the European Data Protection Board (EDPB), such that the case was dealt with by the local data protection authority. In general, the General Data Protection Regulation (GDPR) designates the data protection authority (DPA) of the member state in which a company or organisation has its "main establishment" as the lead supervisory authority. The lead supervisory authority has primary responsibility for overseeing the organisation's compliance with the GDPR across the European Union (EU). However, there are certain circumstances where other DPAs may be responsible. For example, if a data subject files a complaint with a DPA in a member state other than the member state where the data controller or processor has its main establishment, that DPA may have jurisdiction to investigate and resolve the complaint. Additionally, where a cross-border processing activity affects individuals in multiple member states, the GDPR's "one-stop-shop" mechanism may apply. This mechanism allows for the lead supervisory authority to coordinate with other concerned DPAs to reach a joint decision on the matter.

[14] See: https://www.bloomberg.com/news/articles/2022-01-18/eu-s-tough-data-privacy-rules-rake-in-biggest-annual-fines#xj4y7vzkg and https://edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention_en.

Data Protection Review Court, and strong obligations for U.S. companies processing EU data. The framework is subject to periodic reviews to ensure its effective implementation and compliance with EU data protection standards (European Commission, 2023a).

#### *2.1.4 GDPR Data Breach Notification*

According to GDPR (Article 33[15]), a company is required to notify a data protection authority (DPA) of a security breach that affects personal data within 72 hours of becoming aware of the violation. This timing is interpreted as "when feasible," it is thus permissible to ask for a delay and acceptable to notify the DPA gradually as more information about the breach becomes available. Failure to report a breach may result in a punishment of up to EUR 10 million or 2% of the company's annual revenue, whichever is the highest.[16]

The notification should be made to the supervisory authority in the member state where the controller has its main establishment or, if the controller does not have a main establishment in the EU, to the supervisory authority in the member state where the data breach occurred. In addition to notifying the supervisory authority, if the personal data breach is likely to result in a high risk to the rights and freedoms of the data subjects, the controller must also communicate the personal data breach to the data subjects without undue delay.

In 2018, the Marriott hotel chain suffered a data breach that affected up to 500 million customers. The breach was caused by hackers who gained access to the company's Starwood reservation system and stole personal information, including names, addresses, phone numbers, passport numbers, and credit card information. The breach had a significant impact on the affected individuals. It resulted in hefty fines and penalties for the company under GDPR, which highlights the importance of ensuring the security of personal data.

### 2.2 The Network and Information Systems (NIS) Directive

The NIS Directive (EU 2016/1148) was the first cybersecurity law that applies to the entire EU. This Directive admitted, departing from the prior voluntary approach to cybersecurity, that the EU was not adequately protected against security incidents and threats and established a consistent legal framework for cybersecurity in Europe.[17] (ENISA, 2020). The Directive, which is a crucial component of the EU's cybersecurity policy, was adopted by the European Parliament in 2016 and the member states were given 21 months to transpose it into national law.

The NIS Directive represents a crucial step toward a more streamlined EU strategy. It imposes protection responsibilities on Operators of Essential Services (OES) and Data Service Providers (DSPs), which also include search engines, cloud computing services, and online marketplaces. The so-called

[15] Outlines the requirements for notification of a personal data breach to the supervisory authority.
[16] See: https://gdpr-text.com/read/article-33/.
[17] The directive is expected to be replaced by NIS2 by the end of 2024.

essential services comprise those that are crucial to the economy and largely rely on ICT, such as those offered by the banking sector, utilities (energy and industries), financial market infrastructure, health sector, and transport.[18] The Directive only applies to OES and DSPs that provide services within the EU (European Commission, 2022b). The "one-stop shop" approach ensures that DSPs are only subject to the jurisdiction of one regulator within the EU, namely the one in the country where the DSP has its main establishment, and places less strict regulations on DSPs than it does on OES (the providers of vital services).[19] According to the NIS Directive's main requirements, all member states are obliged to adopt a national strategy on the security of network and information systems, and name one or more Computer Security Emergency Response Teams (also called CSIRTs) and a national authority that is in charge of cybersecurity. Furthermore, they must establish a cooperation group to encourage and facilitate information sharing and strategic cooperation among member states through a network of CSIRTs. The Directive intends to achieve a high common degree of security for network and information systems throughout the EU (ENISA, 2020).

Organisations are required to share and disclose information under the NIS Directive when incidents have a "major" or "substantial" impact on service continuity.[20] The European Commission has established guidelines for determining whether or not an incident has a substantial impact on DSPs, and the national regulators are responsible for setting the thresholds for when an incident has "major disruptive consequences" on OES[21] (Michels & Walden, 2018).[22]

The GDPR and the NIS Directives are designed to complement each other, with the GDPR providing specific requirements for the protection of personal data, and the NIS Directive offering a more general framework for the security of network and information systems. Organisations that are subject to both regulations must comply with the requirements of both Directives. Given that the GDPR and NIS Directives create different regulatory bodies, one wonders whether having a single point of contact in the EU for notifications of data breachers and cyberattacks to alert the proper authorities would not enhance efficiency.

[18] Which organisations fall under the definition of 'operator of essential services' is left to each individual member state.

[19] The one-stop-shop principle does not apply to Operators of Essential Services (OES) under the NIS Directive (EU 2016/1148). Instead, each EU member state must designate a competent national authority to oversee the implementation and enforcement of the NIS Directive within its territory for OES. The national authorities (e.g., BSI in Germany, ANSSI in France, DIS in Italy) are responsible for receiving incident reports from the OES, for conducting risk assessments, and for imposing penalties for non-compliance. The reason for the exclusion of the one-stop-shop principle for the OES under the NIS Directive is that the services provided by OES are critical to the functioning of society and the economy, and therefore, any security incident affecting an OES could have significant cross-border effects. By requiring OES to report security incidents directly to their national authority, the NIS Directive aims to ensure that incidents are addressed quickly and effectively, and that cross-border cooperation takes place where necessary.

[20] Organisations are required to share and disclose information with their competent national authority. In addition, organisations may also need to share information with other relevant authorities or organisations, such as sector-specific regulators, other critical infrastructure operators, or law enforcement agencies, depending on the nature and scope of the incident.

[21] To determine the impact of an incident, it is the responsibility of the OES to classify the network and information systems that must comply with the security requirements of the NIS Directive.

[22] Under the NIS2 Directive, the distinction between a DPS and OES will be abandoned.

To address shortcomings in the original framework and respond to the growing threat landscape, the NIS2 Directive (Directive (EU) 2022/2555) was adopted in December 2022 and was to be transposed by Member States into national regulations by 17 October 2024. While many Member States have completed the transposition, some are still in the process of doing so. NIS2 significantly expands the scope of regulation to include more sectors and entities, such as providers of public electronic communications networks, waste management, postal and courier services, manufacturing of critical products, and certain digital infrastructure services. Compared to its predecessor, the NIS Directive (NIS1) that left enforcement and penalties largely to the discretion of individual Member States, the NIS2 introduces a clearer distinction between "essential" and "important" entities, imposes stricter cybersecurity risk management and incident reporting obligations, and harmonises supervisory and enforcement powers across the EU. Penalties for non-compliance can reach up to €10 million or 2% of the global annual turnover. The Directive also strengthens cooperation at EU level through a revamped Cooperation Group and a new EU Cyber Crisis Liaison Organisation Network (EU-CyCLONe), which is responsible for supporting coordinated management of large-scale cybersecurity incidents and crises at the operational level. EU-CyCLONe facilitates information exchange among Member States and ensures situational awareness and response coordination during cross-border cyber emergencies, thereby reinforcing the Union's collective resilience to large-scale cyber threats (ENISA, 2023).
The NIS Directive has established the Network and Information Systems Collaboration Group (NISCG, with its secretariat at the EC) to promote cooperation and information sharing among member states. Representatives of the EU member states and of the EC, and the EU Agency for Cybersecurity (ENISA) constitute the NIS Cooperation Group. The main goal of the Group is to ensure that network and information systems throughout the EU operate at a high level of shared security and that information sharing and strategic cooperation among EU members is enhanced and shared in frequent meetings. The NIS Cooperation Group's operational activities are aided by the network of Computer Security Incident Response Teams (CSIRTs), which are tasked with exchanging knowledge about potential dangers and current security threats as well as addressing specific cybersecurity incidents. Under a new joint operational structure established as a part of the European Democracy Action plan, the NIS Cooperation Group is also closely collaborating with the European Cooperation Network on Elections to address the risks to democratic processes (European Commission, 2022e). The NIS Directive is enforced by national regulatory authorities (NRAs) in each EU member state.

### 2.3 GDPR and NIS as Complementary Frameworks for Protecting Personal Data and Network Security

While both the GDPR and the NIS Directive concern the protection of personal data and the security of networks and information systems, they have different areas of focus and aims, and are not likely to collide. The goal of both regulations is to provide proper data protection and guarantee confidentiality. The NIS Directive is entirely concerned with network security and requires operators to appropriately

secure their networks to assure the delivery of services, whereas the GDPR's goal is to protect personal data (Saqib, Germanos, Zeng & Maglaras, 2020). Different standards are used by the GDPR and NIS to assess what constitutes technological and operational controls (with much more specific information provided under NIS regulations' implementations). However, both the GDPR and the NIS Directive frequently apply to the same situations and have substantial overlap, although the protection mechanisms can differ. In the case of DSPs, the NIS Directive applies only to those with 50 or more employees and whose services are "essential for the maintenance of critical societal and/or economic activities" or "whose main activity consists of the provision of an information society service." This means that only larger DSPs that provide critical or essential services, such as online marketplaces or cloud computing services, are subject to the NIS Directive, hence, a resemblance (to GDPR) only exists in relation to these operators.

The NIS reporting plan is significantly more complicated than the duty to reveal personal data breaches under the GDPR, but organisations that request or require.[23] NIS monitoring are also often also subject to the GDPR reporting requirements. Both regulations have procedures for reporting events, and both laws require operators to use risk-based security measures.

The NIS Directive acknowledges that different industries require different levels of security. Consequently, when implementing the Directive, member states are urged to consider both cross-sectoral and industry-specific issues. As a result, national transpositions of the Directive, even while the security standards generally coincide with those of the GDPR, can offer more detailed requirements than the GDPR (which hinges on the simple requirement of "appropriateness" in taking cybersecurity measures). With regard to breach notification, the GDPR mandates only disclosure in cases where personal data is at risk, whereas the NIS Directive requires disclosure if the cyber-related service is significantly disrupted.

The OES and DSPs (that often act as data processors) must be aware of the variations in the categories of notifiable events, timelines, and competent authorities (also considering that additional

[23] Organisations may request or require NIS monitoring, depending on their specific needs and regulatory requirements. In some cases, organisations may request NIS monitoring as part of their own internal security policies and procedures. This may be done to detect and prevent cyberattacks, data breaches, or other security incidents that could compromise the confidentiality, integrity, or availability of their network and information systems. On the other hand, some organisations may be required by law or regulatory standards to implement NIS monitoring. For example, certain industries such as healthcare, finance, and governmental may be subject to specific regulations or standards that mandate NIS monitoring to ensure compliance and protect sensitive information. Ultimately, whether an organisation requests or requires NIS monitoring depends on its unique circumstances and risk profile. However, given the increasing frequency and severity of cyber threats, many organisations are recognizing the importance of implementing robust NIS monitoring solutions to protect their critical assets and maintain business continuity.

incident reporting duties may exist under national legislation) (Schmitz-Berndt & Anheier, 2021).[24] The problem that an institution may be obliged to notify two different authorities of the same incident has not been resolved. If the notification requirements are not met, a risk of cumulative administrative sanctions occurs, as supervisory authorities under both regimes (NIS and GDPR) may impose penalties for different aspects of the same incident. There is a real possibility of this issue occurring because in the majority of cyber incidents reporting is required under both regulations. The fact that the punishments by different supervisory agencies address different aspects of the violation can be a basis to punish an entity twice for the same incident (e.g., for violations regarding the integrity of the service and the protection of personal data). Given the potential severity of the penalties, businesses could be subject to a maximum fine of twice EUR 20 million for a single event (or twice 4% of their gross revenues). Although the potential severity of the penalty may encourage a change in behaviour, the possibility of double jeopardy may also deter voluntary reporting. In this respect, it is important to recognise that the risk of double jeopardy extends beyond the NIS Directive and the GDPR to other laws focussing on cyber protection of specific industries (e.g., health, finance) (European Commission, 2020).

### 2.4 The EU Agency for Cybersecurity and the Cybersecurity Act

The mission of the European Union Agency for Cybersecurity (also called ENISA after the original name European Union Information Security Agency (used until 2019), which was founded in 2004 (EC 460/2004), is to strengthen operational collaboration between member states at the EU level, to support the coordination of the EU in the event of significant cross-border cyberattacks and crises, and to assist EU member states (if they request so) to address their cybersecurity incidents. The NIS Directive gave ENISA the responsibility of serving as the network's secretariat for national Computer Security Incidents Response Teams (CSIRTs) (European Commission, 2022c).

The EU Cybersecurity Act (EU) 2019/881 gave ENISA a permanent mandate, increased its funding, and added more responsibilities by laying the technical foundation for certification schemes. The certification system refers to a process of verifying and attesting that a product, service, or process meets specific cybersecurity requirements.[25] This Act thus supplements the NIS Directive and was another significant step towards boosting cybersecurity.[26] The certification schemes established under

[24] In Germany for example, the NIS Directive is implemented and enforced by the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, or BSI). The BSI is also responsible for providing technical assistance and guidance to OES and DSPs on how to comply with the Directive. The BSI also has the authority to conduct audits and investigations to ensure compliance with the NIS Directive and to take enforcement action against OESs and DSPs that fail to meet the Directive's obligations. This can include the issue of warnings, orders to take corrective action, and the imposition of fines for non-compliance. In addition to the BSI, other authorities in Germany, such as the Federal Network Agency (Bundesnetzagentur) and the Federal Office for Goods Transport (Bundesanstalt für Güterverkehr) also have the responsibility to enforce the NIS Directive in their respective sectors.

[25] These certificates are not related to encrypting certificates but are product or service certificates that demonstrate a certain level of cybersecurity protection.

[26] See: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

the EU Cybersecurity Act provide a framework for evaluating the cybersecurity of products, services, and processes, and ensuring that they meet certain security standards. The certificates issued under these schemes are intended to demonstrate to customers, regulators, and other stakeholders that the certified products, services, or processes meet the security requirements. Furthermore, the certification schemes cover various domains, including cloud computing services, the internet of things (IoT) devices, and other critical infrastructure systems. The certification process involves a rigorous assessment of the security features and capabilities of the product or service, as well as an evaluation of its ability to resist cyberattacks and protect against other cybersecurity risks.

ENISA does not only play a crucial part in creating and sustaining the European cybersecurity certification framework but is also responsible to notify the public about the certification programs and the certificates granted.[27] In this context, the Cybersecurity Act introduces a framework for cybersecurity certification for Information and Communication Technology (ICT) products, services, and processes. Businesses operating in the EU gain from having to certify their ICT goods, processes, and services, and from having their credentials officially recognized throughout the EU[28] (European Commission, 2022d). ENISA's task is mainly to support public institutions, such as EU authorities, decentralized bodies, or agencies, but also to help the information technology industry, including small and medium businesses, and to conduct academic research. To this end, the NIS Directive, and the Cybersecurity Act (EU 2019/881) provide the legal framework for ENISA's tasks. European countries also have their own national cybersecurity offices; for instance, the Federal Office for Information Security (FOIS) and the Network and Information Security Agency (ANSSI) are the respective German and French agencies.

### 2.4 Laws to Address Specific Industry Vulnerabilities

The European Directives are typically applied by the member states with the power of direct effect, which means that the national authorities must ensure that EU laws are properly applied at the country

[27] As per the EU Cybersecurity Act (EU) 2019/881, ENISA is responsible for maintaining a list of all the certified products, services, and processes, as well as the certification bodies authorized to issue certificates under the European cybersecurity certification framework. The information about the certification programs and the granted certificates can be found on ENISA's website, where a publicly accessible repository of all certified products, services, and processes is maintained. This repository is called the "European Cybersecurity Certification Catalogue" and contains information about the certified products, their certification levels, the certification bodies that issued the certificates, and the certification schemes under which the certificates were issued. Moreover, ENISA is also responsible for disseminating information about the certification schemes and the granted certificates to the public, particularly to the relevant stakeholders, such as regulators, industry, and end-users. ENISA achieves this through various means, such as publishing reports, organizing conferences, workshops, and training sessions, and collaborating with national authorities and industry associations.

[28] Non-binding initiatives such as TIBER-EU (framework for threat intelligence-based ethical red-teaming) were created to establish a framework for threat intelligence to improve the cyber resilience of entities across the continent (ECB, 2022).

level (see above in section 2.7 Enforcement Agencies).[29] In the context of the NIS Directive, this implies that every (industry-specific) state regulator should oversee the Directive's implementation. Additional national regulations could be imposed when the corporate landscape and national needs demand so. By requiring member states to be adequately prepared, the Directive establishes legal measures to increase the overall level of cybersecurity in the EU.[30] A security-conscious culture across industries (including the utilities, transport, banking, financial market infrastructures, healthcare, and digital infrastructures) are essential to protect society and the economy (European Commission, 2022f). At the European level, several regulatory bodies and information sharing frameworks – some are non-binding - exist to address industry-specific needs. Specific sectors that are particularly at risk and need extra protection are:

### *2.4.1 Critical Infrastructure*

In 2020, the EC suggested to adopt new regulations to strengthen the resilience of essential organisations as a crucial component of the EU's work to create a Security Union. The EU works towards an updated and comprehensive legal framework to strengthen both the physical and cyber resilience of critical infrastructure by means of the Directive on the Resilience of Critical Infrastructure (Directive (EU) 2018/1148)[31] and the draft of the revised Directive on the Network and Information Systems (NIS2 (EU 2022/2555).[32] In three core areas - preparedness, reaction, and international cooperation - the draft recommendation intends to maximize and expedite the work to preserve vital infrastructure. It calls for increased support and coordination from the EC to improve reaction and preparedness to existing threats, as well as increased collaboration between member states and with third countries. The vital industries of energy, digital infrastructure, transportation, and space should be given top priority. The EU has a special role to play regarding infrastructure that crosses borders or that

[29] The European Commission proposes new EU laws, the European Parliament and the Council of the European Union adopt them. Once adopted, they become EU laws and are binding on all member states. For example, the European Parliament can propose amendments to a Commission proposal during the legislative process, or it can initiate its own legislative initiative report on a particular topic. If the Parliament decides to propose its own legislation, it will need to go through the same legislative process as any other proposal, including review and approval by the Council of the European Union.

[30] The NIS Cooperation Group is specifically established by the NIS Directive to support and facilitate information sharing and strategic cooperation among member states on network and information security. This is done with the help of a Computer Security Incident Response Team (CSIRT) and a national NIS authority, among other measures required by the Directive.

[31] It was adopted by the EC and EP and came into force in August 2016. Member states were required to transpose the Directive into national law by May 2018. It seeks to enhance the cybersecurity and resilience of critical infrastructure in the EU by setting out common requirements and cooperation mechanisms among member states. Its implementation aims to ensure that critical infrastructure can withstand cyber threats and incidents and continue to provide essential services to society and the economy.

[32] The NIS Directive was introduced to improve the security of networks and information systems for OES and DSPs but some problems with clarity and limited coverage arose (the NIS focused on the banking sector, utilities (energy and industries), financial market infrastructure, health sector, and transport). Therefore, the EC has proposed a new Directive, NIS 2, which eliminates the distinction between OES and DSPs, expands the coverage to new sectors, establishes a European Cyber Crises Liaison Organisation Network (ECCLO), strengthens security requirements for businesses, introduces stricter supervisory measures and aims to harmonize sanctioning regimes across member states. The proposal aims to increase the resilience of various sectors involved, both in the public and private spheres (Schmitz & Cole, 2022).

offers cross-border services and affects the interests of several member states. All member states have an interest in identifying these infrastructure systems as well as the organisations that run them and working together to safeguard them (European Commission, 2022g).

*Energy*

The European Energy Information Sharing & Analysis Centre (EE-ISAC)[33] reinforces the EU power grid's cybersecurity by facilitating the analysis of threats, vulnerabilities, incidents, solutions, and opportunities, by exchanging trustworthy information. To support this proactive information exchange and analysis, and empower its members to take effective actions, the EE-ISAC offers coordination and guidance (European Energy Information Sharing & Analysis Centre, 2022).

*Finance*

The financial industry is extensively regulated, and several EU laws and policies comprise financial cybersecurity rules. Two important directives which include cybersecurity rules are the Revised Payment Services Directive (PSD2, 2015/2366/EU) which regulates payment service providers as well as payment services, and MiFID 2 (2014/65/EU) which provides a framework for the regulation of trading venues, investment intermediaries, and securities markets. Several projects are being implemented by EU institutions, agencies, authorities, regulators, and other stakeholder groups to improve the financial sector's cybersecurity. The EC is accountable for the following activities:

- A FinTech action plan (2018) which promotes better supervisory convergence and implements IT risk management, facilitates information exchange on cyber risks among market participants, and enhances EU cooperation in cyber threat testing by utilizing a single threat-intelligence lead technique, such as TIBER-EU.[34] TIBER-EU is the EU framework for threat intelligence-based ethical red-teaming, which enables the simulation of hostile cyberattacks in order to learn about security vulnerabilities and to provide security feedback thereon. It assists authorities to test and improve the cyber resilience of entities by carrying out a controlled cyberattack.
- The digital finance strategy which aims at reducing fragmentation in the Digital Single Market, modifying the EU regulatory framework to support digital innovation, promoting data-driven finance, addressing the risks and challenges associated with digital transformation, and boosting the financial system's operational digital resilience.
- The Digital Operational Resilience Act (DORA) ((EU) 2022/2554) requires all financial institutions to ensure they are prepared to withstand any dangers or interruptions caused by ICT failure.

[33] It was officially launched in September 2016 by nine European utilities and grid operators.

[34] TIBER-EU is a framework (not a law) developed by the ECB to help financial institutions in the EU to assess and improve their resilience to cyberattacks. It provides a set of guidelines and best practices for conducting controlled and tailored red teaming exercises, which involve ethical hackers attempting to simulate real-world attacks on a financial institution's systems and infrastructure. The use of the TIBER-EU framework is on a voluntary basis and does therefore not have the force of law. Still, it is considered an important tool for enhancing the cyber resilience of financial institutions. Under this framework, the responsibility for conducting ethical hacking, or red teaming, is given to accredited third-party providers, known as TIBER-EU Service Providers, who are selected and supervised by the national central banks of the participating EU member states.

To prevent and mitigate the effects of ICT-related incidents, credit institutions, payment and e-money institutions, insurance companies, and other financial entities must adhere to strict requirements. The Regulation also establishes a framework for monitoring service providers (such as the Big Tech firms) that provide financial entities with essential ICT services (ENISA, 2022a). As DORA is now adopted, it applies directly across all EU Member States from 17 January 2025, without requiring national transposition. ENISA's role will be to support the member states in implementing DORA by providing expertise and guidance on cybersecurity and operational resilience. Specifically, ENISA contributes bydeveloping technical standards and guidelines, delivering training and awareness-raising activities for relevant stakeholders, and facilitating the exchange of best practices and information among the Member States. In addition, DORA introduces unified oversight of critical ICT third-party providers through the European Supervisory Authorities (ESAs), which include the ECB, EBA (European Banking Authority), ESMA, and EIOPA (European Insurance and Occupational Pensions Authority). It sets out comprehensive rules on ICT risk management, incident classification and reporting, digital operational resilience testing, and the management of third-party ICT risk. This regulation marks a significant step toward strengthening the digital resilience of the EU financial sector by ensuring consistent supervisory practices and eliminating national fragmentation (European Union, 2022).

In relation to bank data breaches, the ECB supervises the biggest European banks (smaller banks are supervised by the bank supervision authorities at the national level), and also deals with the banks' IT posture as well as breaches and compliance.[35] Large banks that violate EU law or ECB rulings face financial penalties imposed by the ECB. The ECB may ask the national supervisory authorities (NCAs) to initiate the requisite proceedings in cases of violations of national law implementing EU directives, violations committed by natural persons, or situations where a non-pecuniary penalty must be imposed. According to the relevant national law, the NCA conducts these proceedings and decides on the consequent sanctions (ECB, 2022a). In Addition, the ECB has issued the Cyber Resilience Oversight Expectations (CROE) for financial market infrastructures (FMIs).[36] Based on current global advice, the CROE specifies the regulator's requirements for the Euro-cyber system's resilience and lays out precise instructions for the FMIs on how to adhere to the rules (ENISA, 2022b).

*Healthcare*

Among others, the NIS Directive requires the health sector to have Incident Response Capabilities (IRC).[37] This industry could come under threat at every point in its supply chain, which could have

[35] A big bank is defined by the ECB as a significant institution (SI) when it meets at least one of the following criteria: total assets exceed EUR 30 billion or 20% of the GDP of the member state where it is established. In addition, a credit institution can be identified as an SI by the ECB on the basis of other factors, such as its systemic importance or the extent to which it carries out activities in one or more member states.

[36] Introduced by the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) in June 2016. The CROE provide guidance to regulators and supervisors on how to oversee and assess the cyber resilience of FMIs, such as central counterparties, payment systems, and securities settlement systems.

[37] The IRC is defined as a set of processes, procedures, and resources that an organisation uses to detect, analyse, contain, and recover from cybersecurity incidents.

disastrous societal repercussions for a wide range of stakeholders (citizens, public authorities, regulators, professional associations, large industries, SMEs), the vulnerability of which has been demonstrated at the time of the Covid-19 pandemic. National CSIRTs are the primary organisations in charge of incident response in the healthcare industry, but in all member states, health sectoral CSIRTs are still an exception. However, there is a noticeable tendency towards creating sector-wide CSIRT cooperation, which may involve information sharing and additional activities (ENISA, 2021).

### *2.4.2 National Defence*

In November 2022, the EC sent out a proposed communication for an EU Cyber Defence Policy and an Action Plan on Military Mobility 2.0 to address the deteriorating security situation in the wake of Russia's aggression against Ukraine and to strengthen the EU's ability to safeguard its population and infrastructure.[38] The EU Policy on Cyber Defence seeks to improve EU cyber defence capabilities as well as military and civilian cyber communities' coordination and collaboration (at the level of civilian, law enforcement, diplomacy, and military defence). It is expected to improve the EU's ability to manage cyber crises effectively, assist in reducing reliance on key cyber technologies strategically, and build the European Defence Technological Industrial Base (EDTIB).[39] In addition, it encourages the development, recruitment, and retention of cyber talent, and intensifies collaboration with the partners in the area of cyber defence (European Commission, 2022h).

### *2.4.3 Platform Governance and Digital Services*

The eIDAS (Electronic Identification, Authentication and Trust Services (910/2014)) regulation aims to create a common legal framework for secure electronic transactions across EU member states. The regulation, which came into effect on July 1, 2016, replaces the previous Electronic Signatures Directive (1999/93/EC) and provides new rules for electronic identification, electronic signatures, electronic seals, electronic time stamping, electronic documents, and website authentication (European Commission, 2023a). eIDAS is designed to improve the security and reliability of electronic transactions, increase cross-border interoperability, and enhance trust in the digital economy. It establishes a common set of standards for electronic signatures and authentication mechanisms and enables electronic transactions to be legally recognized across the EU. The regulation also provides a

[38] A Joint Communication (JC) refers to a document that is jointly developed and issued by the EC and the High Representative of the Union for Foreign Affairs and Security Policy. A JC is not legally binding, but it serves as a significant policy document that outlines the EU's position on a particular issue and proposes actions or recommendations to address it. JCs are usually addressed to the EP, the Council of the EU, and other relevant EU institutions, as well as to the EU's partners and stakeholders.

[39] The European Defence Technological and Industrial Base (EDTIB) is a term used to describe the network of European companies, organisations, and research institutes involved in the research, development, production, and maintenance of defence technologies and equipment. It encompasses a wide range of sectors, including aerospace, land systems, naval systems, cyber defence, and advanced materials.

framework for electronic trust services such as electronic registered delivery services, electronic archiving services, and electronic time-stamping services.

Under eIDAS, member states are required to ensure that electronic identification and trust services are provided in a secure, trustworthy, and user-friendly way, and that all EU citizens and businesses have access to these services. The regulation also encourages the development of new electronic identification and trust services and promotes innovation in the digital economy.

Complementing these technical trust mechanisms, the Digital Markets Act (DMA) (Regulation (EU) 2022/1925), which entered into force on 1 November 2022 and became fully applicable on 2 May 2023, introduces ex ante regulatory obligations for large online platforms designated as "gatekeepers." These are firms with significant impact on the internal market that act as intermediaries between business users and end-users. The DMA prohibits practices such as self-preferencing, mandates interoperability with third-party services, and bans the combination of personal data across services without explicit user consent. By promoting market fairness, interoperability, and user choice, the DMA addresses structural imbalances in digital markets and reinforces the data protection principles of the GDPR. The European Commission is the primary enforcement authority and may impose fines of up to 10% of global annual turnover, or 20% for repeat violations (European Commission, 2022).

Building upon these platform-level interventions, the forthcoming Digital Networks Act (DNA) shifts regulatory attention to the foundational layer of digital infrastructure. The DNA, under consultation and expected to be finalised by the end of 2025, represents a significant shift in the EU's regulatory framework for digital infrastructure and connectivity. Unlike the Digital Services Act (DSA) and the Digital Markets Act (DMA), which primarily govern platform behaviour and market competition, the DNA directly targets the telecommunications and electronic communications sector. It is proposed as a Regulation, meaning it will be directly applicable in all Member States without the need for national transposition, ensuring immediate harmonisation across the Union.

The DNA's primary objectives include the coordination of spectrum management, the acceleration of investment in very high-capacity networks (notably 5G and future 6G infrastructure), and the removal of regulatory barriers to network deployment. It seeks to consolidate and update existing telecom laws (notably the European Electronic Communications Code) and address longstanding issues such as market fragmentation, inconsistent rules on access pricing, and delays in spectrum assignment. From a strategic perspective, the DNA is also expected to reinforce the EU's digital sovereignty goals, particularly by improving network resilience, clarifying obligations for cross-border infrastructure deployment, and creating clearer rules for fair contribution mechanisms, whereby large content providers may be required to contribute financially to network maintenance and expansion. While some aspects remain politically contested, the DNA could fundamentally recalibrate the power dynamics between telecom operators, content providers, and national regulators.

As such, the DNA complements existing digital regulation by extending the EU's oversight into the physical layer of digital connectivity, thereby ensuring that the Union's digital ambitions, such

as universal high-speed access, secure infrastructure, and innovation capacity, are supported by a robust, future-proof regulatory framework (European Commission, 2025).

### 2.5 Cross-Border Data Governance: The Free Flow of Non-Personal Data (FFD) Regulation

As digital transformation accelerates, the ability to store, process, and transfer data across borders has become essential for economic activity, innovation, and the deployment of modern IT infrastructure, including cloud computing, AI applications, and data-driven services. However, various EU Member States had previously imposed data localisation requirements, restricting the movement of certain data types to ensure domestic control. These rules created fragmentation and inefficiencies, particularly in cross-border digital services, public sector data use, and cybersecurity coordination.

The Free Flow of Non-Personal Data Regulation (Regulation (EU) 2018/1807), applicable since May 2019, was introduced to eliminate unjustified data localisation restrictions within the EU. It guarantees that non-personal data can move freely across Member States, thereby fostering a more integrated and competitive data economy. At the same time, it ensures that national authorities retain access to data, even when it is stored in another Member State, thereby preserving regulatory oversight and addressing sovereignty concerns.

While the Regulation does not apply to personal data, already covered by the General Data Protection Regulation (GDPR), it is designed to complement the GDPR, enabling a harmonised and secure digital environment for both personal and non-personal data. Together, the FFD Regulation and the GDPR provide a comprehensive legal framework that strengthens data governance, supports cloud adoption, and reinforces the EU's cybersecurity and digital resilience strategy. The FFD Regulation also introduced the concept of self-regulatory codes of conduct to encourage transparent and fair cloud switching and data porting practices across providers, further enhancing user control and interoperability in the digital single market (European Commission, 2023b). A closely related initiative is the Open Data and Public Sector Information (OD-PSI) Directive (Directive (EU) 2019/1024), which focuses specifically on improving access to and reuse of non-personal data held by public sector bodies. The Directive requires Member States to make such data available in machine-readable formats and encourages the development of APIs for interoperability. It also introduces the concept of high-value datasets, including geospatial, environmental, and mobility data, which must be made available free of charge and with minimal restrictions. Although the Directive does not directly address cybersecurity or personal data protection, it plays a key role in supporting the EU's data-driven economy, and complements both the GDPR and the FFD Regulation by fostering transparent, open, and innovation-friendly use of public sector data (European Commission, 2019).

### 2.6 Data Sharing and Reuse Frameworks: Data Governance Act (DGA)

The Data Governance Act ((EU) 2022/868) is a crucial tenet of the European data strategy and aims to strengthen procedures for increasing data availability, fostering trust in data sharing, and removing technical barriers to reuse. The establishment and growth of common European data spaces in strategic domains, involving both public and private players, will also be fostered by this Act. These strategic domains include the sectors related to health, environment, energy, agriculture, mobility, finance, manufacturing, skills, and public administration. To maximize the potential of data for European consumers and businesses, the Act intends to increase the amount of data available and promote data sharing across industries and EU member states. Through four major types of initiatives, the EU will promote the creation of reliable data-sharing systems and develop:

- Measures to guarantee that, inside the common European data spaces, data intermediaries will serve as reliable coordinators of data sharing or pooling.
- Measures that make it easier for people to share data, particularly those who enable data to be used across industries and countries, as well as simplify the finding of appropriate data for a given user.
- Mechanisms to facilitate the reuse of specific public sector data that is not permitted to be made publicly available. Repurposing health data, for instance, could assist efforts to develop treatments for uncommon or persistent diseases.
- Measures to simplify the process of citizens and companies making their data available (European Commission, 2022i).

Although the Act is not primarily a cybersecurity regulation, it has direct implications for cyber resilience: by promoting trusted data intermediaries and secure mechanisms for sharing sensitive data, it places an implicit obligation on companies and public sector bodies to ensure strong data protection and cybersecurity safeguards. Companies acting as data intermediaries or re-users of protected public-sector data must implement appropriate technical and organisational security measures to comply with the trust framework envisioned by the regulation.

### 2.7 Legal Work in Progress: New Initiatives

The EC now intends to lay a stronger legal foundation for European data and cybersecurity law by means of a comprehensive package of measures. The main ongoing initiatives are:

#### *2.7.1 The Cyber Resilience Act*[40]

[40] Although the CRA has entered into force, it is considered a legal work in progress because its obligations will only begin to apply from December 2027, giving stakeholders a transitional period to adapt technical, legal, and organisational processes to the new requirements.

Products and software with digital components are rife in daily life. The security risk that such devices and software may bring is substantial, although possibly less conspicuous.[41] The new Cyber Resilience Act (CRA) ((EU) 2024/2847), adopted by the European Union in December 2024, establishes a comprehensive legal framework to protect consumers and companies using or purchasing products with digital elements, including both hardware with embedded software and standalone software. Examples of affected products include consumer products such as smartphones, mobile apps, internet-connected toys, but also industrial products such as accounting software, smart meters, or automation devices. The overarching objective of this Act is to implement a minimum level of cybersecurity within the EU market. It covers all phases of the product lifecycle, from design and development to maintenance and end-of-life.[42] The regulation addresses two key issues: (i) the widespread presence of built-in cybersecurity flaws and lack of timely updates; and (ii) the lack of transparency for customers and companies in assessing the cyber robustness of these products. By enforcing a duty of care throughout the product's lifecycle and imposing tiered obligations based on product criticality, the CRA aims to ensure that digital products are secure-by-design and subject to harmonised rules across the Single Market. The Act primarily affects manufacturers, developers, and distributors of products with digital components, who must now integrate cybersecurity features from the outset, ensure ongoing security support through updates, and provide clear information on cyber risks and compliance. The first obligations will apply from December 2027, with enforcement powers and penalties of up to €15 million or 2.5% of global annual turnover for non-compliance (European Commission, 2024).

### *2.7.2 The Artificial Intelligence Act[43]*

Artificial Intelligence (Regulation (EU) 2024/1689) has a substantial impact on a variety of aspects of people's lives, as it is already used to detect cancer, tailor online content, or analyse facial data to enforce laws or personalize adverts. The Act was adopted in March 2024 with the intention of creating a framework for the moral development, application, and deployment of AI within the EU. The Act is intended to support the ethical development and application of AI while simultaneously defending people's rights and interests. Transparency, non-discrimination, and fairness are just a few of the key principles that must be observed when creating and utilizing AI. It classifies AI systems by risk level - unacceptable, high, limited, and minimal, and imposes obligations accordingly. High-risk AI applications are subject to strict requirements, including documentation, human oversight, and, where

[41] This includes the potential for data leakage through seemingly innocuous devices, such as printers and photocopiers.
[42] Software with a digital component generally refers to any computer program or application that utilizes digital technology as a core part of its functionality. It also includes software that is designed to work with digital data, such as binary code or digital files, and may also interact with other digital devices or systems.
[43] Although the Act has been formally adopted, most of its provisions will only apply gradually over the coming years, with key obligations for high-risk systems entering into force up to 24 months after adoption. This phased implementation is why the regulation is still considered a legal work in progress.

applicable, conformity assessment procedures (European Commission, 2022j). Companies placing high-risk AI systems on the EU market must implement risk management systems, maintain technical documentation, ensure transparency toward users, enable human oversight, and undergo independent conformity assessment, either internally or, for certain critical applications, by accredited notified bodies designated by EU Member States, prior to deployment. Non-compliance may lead to significant administrative fines, depending on the severity of the violation.

### *2.7.3 The Data Act (DA)*

The Data Act ((EU) 2023/2854) (applicable from September 2025) focuses on who can access and utilize data collected in the EU across all economic sectors for value creation, and under what circumstances this can occur. It should be noted that the Data Governance Act (EU 2022/868) establishes the procedures and frameworks to facilitate the use of data. The DA aims to ensure fair access to data generated in the EU, stimulate a competitive data market, promote data-driven innovation, and make data more accessible to all. The proposed act includes measures to allow users of connected devices to access and share data, protect small and medium sized enterprises (SMEs) from unfair contractual terms, provide public sector bodies with necessary information, and allow customers to switch between different cloud data-processing service providers. The act also reviews some aspects of the Database Directive[44], namely a clarification that databases containing IoT data should not be subject to separate legal protection. The act is expected to benefit both consumers and businesses, enabling them to make better decisions and benefit from a more competitive data market. The regulation applies from 12 September 2025 (European Commission, 2022k). Although not a cybersecurity law per se, the Data Act has strong cyber-related implications. It requires companies - particularly manufacturers of connected devices and cloud service providers, to implement robust access controls, data-sharing safeguards, and secure-by-design mechanisms. The obligation to make data more accessible and portable across providers raises additional responsibilities for protecting data in transit and storage. As such, firms must strengthen their cybersecurity posture to comply with new obligations around data integrity, confidentiality, and cross-provider transfers.

### *2.7.4 EUCC Certification Scheme*

In January 2024, the European Commission adopted Regulation (EU) 2024/482, establishing the European Common Criteria-based Certification Scheme (EUCC) as a delegated act under the Cybersecurity Act (Regulation (EU) 2019/881). The EUCC introduces a voluntary cybersecurity

[44] The DBD (Directive 96/9/EC) establishes a framework for the legal protection of databases. It provides for a two-tiered protection system, where the structure and organisation of a database may be protected by copyright, while the contents of the database may be protected by a sui generis right (a special type of intellectual property right). The Directive harmonizes the legal protection of databases across the EU, providing legal certainty and protection for creators and users alike. Transposed into the national laws of all EU member states, the Directive has had a significant impact on the development of the European database industry.

certification framework for ICT products with digital elements, including smartcards, firewalls, routers, secure microcontrollers, and similar hardware and software components. The scheme draws from the internationally recognised Common Criteria (ISO/IEC 15408) and establishes assurance levels (from AVA_VAN.1 to AVA_VAN.5) to reflect increasing degrees of resistance against known and unknown attack methods.

By replacing the earlier SOG-IS agreement, the EUCC creates a harmonised internal market mechanism for recognising ICT certifications across the EU, aiming to reduce fragmentation and facilitate cross-border procurement and regulatory interoperability. It enables manufacturers to undergo one certification process that is valid EU-wide, provided it is issued by a national certification authority accredited under ENISA oversight. Although the scheme remains voluntary, it is expected to become a de facto requirement for suppliers bidding in public procurement or operating in high-risk sectors (such as defence, finance, and health), where certified security assurance is essential.

The EUCC is part of the EU's broader effort to institutionalise "security by design" principles and encourage transparent product development lifecycles. It complements the Cyber Resilience Act, which targets consumer-facing digital products and imposes mandatory cybersecurity requirements. Together, these instruments advance the strategic goal of enhancing cybersecurity trust, market integrity, and digital sovereignty in the Union (European Commission, 2024).

## 3. U.S. Regulation

In contrast to the EU's GDPR, the U.S. lacks comprehensive federal legislation governing privacy and cybersecurity and has largely left regulation to the individual states. The federal initiatives have been focused on enhancing cybersecurity for specific industries. Although there is no comprehensive federal data breach notification regulation, several federal statutes do compel data breach notifications in specific circumstances. Examples are the Federal Trade Commission Act (FTC Act; already enacted in 1914), the Financial Services Modernization Act (Gramm-Leach-Bliley Act, 1999), the Health Insurance Portability and Accountability Act (HIPAA, 1996) (Daly, 2018), or the 2002 Homeland Security Act.

### 3.1 General Cybersecurity Regulation

In the federal and international fora, the 2002 Homeland Security Act provides the mandate to investigate a hostile cyber activity, promote cybersecurity, and increase cybersecurity resilience across the U.S. This government-wide initiative to understand, control, and lower danger to digital infrastructure is led by the Cybersecurity and Infrastructure Security Agency (CISA) which operates under the Department of Homeland Security and was established by the Cybersecurity and Infrastructure Security Act of 2018. The agency supports both public and private stakeholders by providing information, analysis, and tools to make them enhance their physical, cyber, and

communications security and resilience. The federal government, state, local, tribal, and territorial authorities, the private sector, and international partners collaborate and exchange cyber defence information through CISA, which performs two main operational tasks. First, in close collaboration with the Office of Management and Budget, the Office of the National Cyber Director, and the Chief Information Officers and Chief Information Security Officers of federal agencies, CISA is responsible for protecting and defending federal civilian executive branch networks as the operational lead for federal cybersecurity. Second, CISA leads efforts to secure critical infrastructure, working with both governmental and private stakeholders to safeguard essential national systems. The primary areas of attention for CISA[45] are:

- Offering free tools and resources to partners in the public and private sectors;
- Facilitating vulnerability assessments for key infrastructure;
- Improving security and adaptability across the chemical industry;
- Promoting sector alliances, facilitating information sharing, and providing training and international cooperation (Department of Homeland Security, 2022).

The Cybersecurity Information Sharing Act (CISA) of 2015, enacted as Title I of the Cybersecurity Act of 2015, provides the legal foundation for the voluntary exchange of cyber threat indicators and defensive measures between private entities and the federal government. It eliminates legal uncertainty by granting liability protection to organisations that share information in good faith and in compliance with privacy safeguards. The Act designates the Department of Homeland Security as the central recipient of such data and mandates the removal of personal information prior to its exchange. CISA thereby strengthens public–private cooperation on cybersecurity threat intelligence, particularly on the protection of critical infrastructure (U.S. Congress. (2015).

### 3.2 The Definition and Protection of Data Privacy

The current state of data privacy regulation in the U.S. is somewhat fragmented. Although there is no comprehensive federal law governing data privacy, several statutes exist to address specific needs. The Federal Privacy Act of 1974, for example, sets out regulations that govern how federal agencies collect, store, use, and share personally identifiable information. Similarly, the private market is governed by regulations such as the Electronic Communications Privacy Act (1986) and the Stored Communications Act (1986), which respectively restrict unwarranted monitoring and prohibit unauthorized access, disclosure, or use of wire, oral, or electronic communications. In addition, Title

[45] The Department of Homeland Security describes their Cybersecurity efforts at: https://www.dhs.gov/topics/cybersecurity.

18 of the U.S. Code[46] Chapter 119[47] and Chapter 121[48] respectively, deal with restricting unwarranted monitoring, and with prohibiting the unauthorized use, disclosure, or access to any wire, oral, or electronic communication.[49] Although further attempts to regulate cyber breaches at the federal level were made by the Judiciary Committee of Congress in 2003, a proposal was not put to vote. Similarly, the Personal Data Notification & Protection Act (PDNPA) proposed by the Obama administration in 2015 did not pass. Consequently, businesses operating in various states (and internationally) face the issue of compliance with a wide variety of (possibly outdated) privacy and data breach laws (Congress, 2017).

At the federal level and according to the U.S. Department of Labour, personal identifiable information is defined as data that: (i) directly identifies a person (e.g., name, address, social security number, or other identifying number or code, phone number, email address, etc.); or (ii) allows an organisation to indirectly identify particular people by combining their data with other data elements. These informational components may combine gender, race, date of birth, location, and other attributes. Furthermore, information that enables offline or online communication with a particular individual qualifies as personally identifiable information. These data can be kept on paper, electronically, or through other types of media (U.S. Department of Labor, 2022).

Likewise, the definition of personal information commonly used in most states is a person's first name, first initial, and last name along with one or more of the data components: (i) social security number; (ii) the number on a driver's license or another government-issued identification card; (iii) a bank account number, credit card number, or debit card number along with any security code, access code, PIN code, or password required to access an account. Information that is legally made available to the public through federal, state, or local government documents or widely circulated media is not considered to be personal information. Furthermore, a data breach is commonly defined as the wrongful or unauthorized acquisition of personal data that jeopardizes its integrity, security, or secrecy (Garrison & Hamilton, 2019).

### 3.3 State Legislation on Privacy

In addition to federal regulation, laws in each of the 50 states mandate individuals, companies, and governmental organisations to warn victims of data security breaches involving personally identifiable information. The majority of security breach laws include provisions on who must abide by the law (such as businesses, data or information brokers, government entities, etc.), what constitutes personal

[46] The U.S. Code is a compilation and codification of federal laws into 54 titles, each representing a broad subject area of federal law. The Code comprises all general and permanent federal laws enacted by Congress and approved by the President, as well as related statutes and treaties.
[47] Called the Wiretap Act
[48] Called the Stored Communications Act (SCA)
[49] The United States Code is a compilation of federal laws of the U.S. it codifies the general and permanent laws and organises them into 54 titles covering a wide range of topics, including criminal law, civil rights, intellectual property, tax law, and more. Both the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA) are part of the U.S. Code.

information, what constitutes a breach (such as the unauthorized acquisition of data), how to notify the appropriate parties, and what are the exemptions (e.g., for encrypted information) (NCSL, 2022). State laws are subordinate to federal regulation in case of conflict due to the Supremacy Clause of the Constitution (U.S. Const. art. VI., § 2) (Legal Information Institute, 2022b). However, as a consequence of the lack of a comprehensive federal law on data privacy, security breach notification laws at the state level prevail.

A state legislates to set a standard for businesses within its borders, to protect the quality of living of its inhabitants, but when a company within a state serves clients outside this state, the state law applies to those out-of-state clients as well. There is substantial heterogeneity among states in terms of the severity of notification laws (see Appendix 3). For instance, residents of California have the right to know, under the California Consumer Privacy Act (2020), what their personal information is used for and how this is used. They can demand that a corporation erase their personal information at any time. Consumers are also informed about which third-party organisations receive their personal information and have the option to deny the selling of their data.[50] While California was the first state to enact a data breach notification law (in 2002), most states have followed California's lead by also legally enforcing the disclosure of data breaches. However, these state-level Data Breach Notification Laws substantially differ in terms of reporting thresholds (e.g., the number of individuals affected), the definition of personal information that is violated, and the fines for non-compliance (Daly, 2018). While in South Carolina the penalty for violation stands at USD 1,000 per breach that affect at least 1000 individuals, in other states the penalty is higher, e.g., in Michigan, it exceeds USD 500,000 for the same number of individuals. In California[51], fines can reach USD 250,000 for a breach affecting a minimum of 500 individuals.[52] State examples of breach thresholds are Oregon where a breached entity must report when more than 250 individuals' privacy was breached, whereas in Georgia, the minimum threshold stands at 10,000 individuals. Also, breach notification laws were introduced gradually across states; among the lagging states are Alabama and South Dakota, which introduced breach notification laws as late as 2018.

Each state has adopted a specific enforcement approach, which manifests itself in the varying numbers of breach incidents reported per state. Appendix 3 provides an overview of all cyber-related state-level rules.

Even if a breached entity has duly reported an incident and has been compliant with its state law, affected parties can still bring a data breach lawsuit against the entity. To successfully do so, the plaintiff must demonstrate that the entity was negligent and violated the U.S. data breach laws.[53] An example is

[50] See https://www.techtarget.com/searchsecurity/news/252513259/Why-Massachusetts-data-breach-reports-are-so-high.
[51] Data or assets that have been exposed include personal financial identity (PFI) such as credit card details, and personal identity information (PII) e.g., social security numbers.
[52] Intentional violations of the state's privacy act can also bring civil penalties in a lawsuit brought by the Attorney General.
[53] See: https://www.myinjuryattorney.com/consumer-privacy-data-breach-lawyers/can-i-be-compensated-after-a-data-breach/#:~:text=Can%20I%20Sue%20a%20Company,United%20States%20data%20breach%20laws.

Sifuentes v. Dropbox Inc., where the plaintiff filed an action against Dropbox alleging his account was compromised in a 2012 data breach,[54] when Dropbox was hacked and more than 68 million users' data and passwords were leaked.[55] The plaintiff alleged that Dropbox failed to notify the problem and as a result, his bank account had been made vulnerable and personal information could have been abused. On the grounds of these facts, the plaintiff sued for invasion of privacy by public disclosure, negligence[56], internal infliction of emotional distress, as well as the breach of the Fair Credit Reporting Act (1970), the Fair, and Accurate Credit Transactions Act (of 2003), the Michigan Law section 445.72[57], and the California Civil Code 1798.29 (which is the state's privacy breach notification law)[58]. This example shows how notification laws are intertwined with other rules of negligence and consumer protection for providing safe grounds for personal data online.

Another example of data breach investigation and litigation is the Capital One incident which revealed that the company did not put in place the necessary security controls. The litigation process also showed that the National Institute of Standards and Technology (NIST) Framework[59], the set of guidelines for mitigating organisational cybersecurity risks, would have been adequate to mitigate the situation. Then, the compliance controls would have spotted unauthorized access and data exfiltration.

It is assumed that criminal code and laws governing armed conflicts are not sufficient to deal with the importance and complexity of cybersecurity. It is thus necessary to develop a strategy that can take into account the widespread pattern of underinvestment in cyber-defence among companies. Since companies do not pay the entire costs of the cyberattacks - some of the harm is externalized onto third parties, these firms occasionally fail to sufficiently defend their systems against attackers. Companies may also have lower incentives to invest in cyber-security because of free-rider problems: by strengthening their cyber defences, they help to secure the systems of others who thus benefit from such cyber-security investments (Sales, 2013; Kosseff, 2016).

Limitations of tort law can also be seen in the litigation case of a credit union against a retailer (Cumis Insurance Society Inc. v. BJ Wholesale Club Inc. (2009)), in which hackers gained access to the retailer's computer systems and stole customer credit card information in 2009. The Supreme

[54] See: https://www.casemine.com/judgement/us/62c3bf3cb50db96bc1b64ec0#.
[55] See: https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach#:~:text=Popular%20cloud%20storage%20firm%20Dropbox,had%20been%20stolen%20as%20well.
[56] The negligence theory and analysis require a comparison of responsibilities in the action that is thought to have violated the appropriate standard of care, to determine carelessness. According to the Third Restatement of Torts (series of legal treatises that provide guidance on the common law in various areas of law, including torts), "primary factors to consider in ascertaining whether the person's conduct lacks reasonable care are the foreseeable likelihood that the person's conduct will result in harm, the foreseeable severity of any harm that may ensue, and the burden of precautions to eliminate or reduce the risk of harm" (Lunn, 2014).
[57] Michigan Law Section 445.72 is a part of the Michigan Consumer Protection Act (MCPA), a civil law.
[58] See: https://www.casemine.com/judgement/us/62c3bf3cb50db96bc1b64ec0#.
[59] The NIST Framework, aka NIST Cybersecurity Framework, is a set of guidelines and best practices for organisations to manage and reduce cybersecurity risks. It was developed by NIST, which is a part of the U.S. Department of Commerce. The framework is widely used by organisations in both the public and private sectors to improve their cybersecurity posture. It is a flexible and scalable framework that can be customized to meet the unique needs of individual organisations. The framework has also been adopted by many governments and industry sectors around the world as a best practice for cybersecurity risk management (Shackelford et al., 2015; Ferraro, 2020).

Judicial Court of Massachusetts concurred with the lower court's judgement that the "economic loss theory prevented compensation on their negligence claims" because "the plaintiffs incurred solely economic harm due to the theft of the credit card account information" (Sales, 2013). This demonstrates that some cyber incidents fall under negligence law, and strict liability might be applied in case of physical damage. Negligence requires proof that the injurer failed to exercise due care, while strict liability imposes responsibility for harm regardless of fault (Schaefer & Mueller-Langer, 2008). In cybersecurity, strict liability could apply where harm stems from inherently dangerous digital practices or regulated failures.

### *3.4 Examples of Litigation*

The class action settlement relating to the infamously large Equifax data breach in September 2017, in which personal and financial information of 147 million Americans was lost, was settled on January 13, 2020. The initial settlement fund contained USD 380 million, with an additional USD 125 million available to cover any out-of-pocket damages[60]. The court-approved class settlement additionally mandated that Equifax pay "possibly USD 2 billion more if all 147 million class members sign up for credit monitoring".[61] Equifax is by no means an isolated case; numerous well-known companies have faced consumer class action lawsuits in the last ten years for breaking data privacy rules (such as e.g. the Fair Credit Reporting Act or FCRA), primarily under U.S. federal laws such as the Fair Credit Reporting Act (FCRA), and not necessarily under state-level legislation. Home Depot (fined USD 200 million), Capital One (USD 190 m), Uber (USD 148 m), Morgan Stanley (USD 120 m), and Yahoo! (USD 85 m) are just a few of the companies that have settled data breach class lawsuits.[62] These cases reflect general privacy breaches and cybersecurity lapses that triggered federal enforcement or large-scale class actions, and they illustrate the growing legal exposure companies face following major data breaches.

### 3.5 Supervisory Bodies

To enforce the federal privacy and cyber risk regulations, a host of institutions are allotted supervisory power. The FTC enforces several key statutes related to privacy and data security, including the FTCA (§5, 15 U.S. Code § 45), which prohibits unfair or deceptive practices; the Gramm-Leach-

[60] Out-of-pocket damages refer to expenses that an individual or organisation incurs as a result of a particular event or incident. These expenses are not covered by insurance or any other third-party source and must be paid directly by the individual or organisation affected.

[61] Under the terms of the settlement, Equifax agreed to provide affected individuals with credit monitoring and identity theft protection services for up to 10 years. If all 147 million class members sign up for these services, Equifax will pay up to USD 2 billion to cover the costs of providing these services. A credit monitoring service keeps track of modifications in borrower conduct and alerts clients to suspected fraud as well as modifications in creditworthiness.

[62] See: https://www.reuters.com/legal/legalindustry/data-breach-class-action-litigation-changing-legal-landscape-2022-06-27/.

Bliley Act (GLBA), under which the FTC enforces the Safeguards Rule establishing cybersecurity standards for financial institutions; and the Children's Online Privacy Protection Act (COPPA), which protects the privacy of children under 13 online. While the Safeguards Rule is issued under GLBA, it complements the FTC's broader authority under the FTCA. These laws are discussed further in the following sections. [63]

Second, the U.S. Department of Justice (DoJ) enforces the Electronic Communications Privacy Act (ECPA) and Stored Communications Act (SCA -18 U.S. Code Chapter 119 and 18 U.S. Code Chapter 121 §§ 2701–2712), both from 1986, which prohibits unwarranted access to communication. The DOJ would have enforced the proposed Consumer Privacy Protection Act of 2017 (CPPA), which aimed to make it unlawful to knowingly and purposefully fail to disclose a security breach that causes any person to suffer an economic loss of at least USD 1,000.[64] The CPPA would have granted the DOJ permission to bring a civil lawsuit in order to: (1) stop ongoing behavior that damages 100 or more protected computers (such as government or corporate computers); and (2) stop the sale of property that was obtained illegally. The act would also have mandated the implementation of a thorough consumer privacy and data security program by commercial companies. When sensitive personally identifiable information (PII) is accessed, obtained, or reasonably thought to have been accessed, acquired, or accessed, a commercial business is required to notify the U.S. residents concerned. Geographic location, password-protected images, and videos, as well as electronic or digital versions of personal, financial, health, and biometric data, are all examples of sensitive PII. The DOJ, the FTC, and the states would have been given the authority to enforce compliance and set civil fines for noncompliance (Congress, H.R.4081 – Consumer Privacy Protection Act of 2017, 2022).

Third, the Department of Homeland Security enforces the 2002 Homeland Security Act (see Section 3.2). Fourth, the Food and Drug Administration (FDA) enforces the Regulations for the Use of Electronic Records in Clinical Investigations of 1997 (21 Code of Federal Regulations (CFR) Part 11), which limits authorized users' access to a system containing sensitive data related to citizen's health and medical research. The FDA only enforces data protection on the industries that falls under its authority: medical device manufacturers, drug producers, biotech companies, biologics developers, and other. Fifth, the Health and Human Services (HHS) Office for Civil Rights (OCR) enforces the Health Insurance Portability and Accountability Act of 1996 (HIPAA - 45 CFR Part 160, and Part 164) which protects sensitive patient health information (see Section 3.10.2).

Six, the U.S. Department of Defence (DoD) enforces the Defence Federal Acquisition Regulation of 1984 (DFAR - 48 CFR 252.204-7012) which holds DoD contractors to specific security standards.

[63] There are various federal bodies responsible for enforcing privacy and cybersecurity regulations in the U.S. These include the Federal Trade Commission (FTC), Department of Health and Human Services (HHS), Federal Communications Commission (FCC), Consumer Financial Protection Bureau (CFPB), and the Department of Justice (DOJ), each with their own specific focus areas such as healthcare information, financial information, and cybercrime. These bodies work together to protect individuals' privacy and cybersecurity under relevant laws and regulations.

[64] Under the CPPA, the U.S. Secret Service and the Federal Bureau of Investigation (FBI) are given permission to conduct investigations into violations, and violators are subject to criminal penalties.

Federal agencies are responsible for enforcing the Privacy Act of 1974 within their respective domains. In the case of healthcare data, the HHS Office for Civil Rights (OCR) enforces HIPAA, which governs medical privacy. Seventh, the Securities and Exchange Commission (SEC) (along with the Financial Industry Regulatory Authority or FINRA) enforces the Securities Act of 1933 that guards the standards of reporting transparency of information related to financial transactions, assets, and markets. It also enforces the CFR (17 CFR Subpart A - Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information) and the Sarbanes-Oxley Act (SOX) of 2002 on corporate governance, which updated parts of the old Securities and Exchange Act. These acts hold public firms to a minimum level of cybersecurity and privacy standards. In the next section, we delve deeper in the responsibilities of the SEC.

### 3.6 The Role of the Securities and Exchange Commission (SEC)

The statutory and regulatory sources for corporate data security requirements are many and varied, including breach notification laws, privacy laws, data security laws, and laws governing electronic transactions and corporate governance (Trautman & Ormerod, 2017). A fundamental act for the financial sector is the Securities Act of 1933, which states that securities buyers should receive complete and accurate information prior to their investment. The Securities Act of 1933 was enacted subsequent to the 1929 stock market crash to protect investors. The act had two main objectives: to establish regulations against deception and fraudulent activity in the securities markets and to ensure more transparency in financial statements so that investors can make educated investment decisions. The act's goal was to enhance corporate financial disclosure and transparency. Therefore, businesses that purposefully fail to report breaches can be held liable.[65]

Regrettably, the legislation falls short as the disclosures it demands are ambiguous, uniform across industries and businesses, and provide little market information. In particular, it fails to address the knowledge asymmetry issue that disclosure regulations are supposed to address between business managers and stockholders. While this criticism applies to much of the cybersecurity legislation, it is focused in particular on the SEC guidance in relation to cyber risks and financial information disclosure in its 2011 Guidelines. It also details when publicly traded companies should disclose information about cybersecurity vulnerabilities and attacks in their annual public filings in response to growing concerns over the threat of cyberattacks on corporate America. Cybersecurity risks are recognized as material information that firms are required to report under current securities law disclosure requirements and accounting standards (Trautman & Ormerod 2017).

The SEC also administers the Sarbanes-Oxley Act (SOX, 2002), which intends to strengthen corporate governance and protect shareholders, investors, and business partners of public companies. SOX and the SEC's 2011 guidelines are the two main legal foundations for corporate governance data

[65] See: https://www.law.cornell.edu/wex/securities_act_of_1933.

security obligations.[66] According to SOX, public firms must implement suitable information security controls for their financial data (Trautman & Newman, 2022). For instance, publicly traded companies must disclose their cybersecurity certifications. As SOX was passed to address the causes of the major scandal of Enron, its primary goals were to enhance internal audits, financial reporting, operational risk measurement, and transparency of business processes in publicly traded corporations. The Act encompasses corporate governance and financial disclosure compliance and sets severe sanctions for failure to follow its rules.[67] SOX has been praised for enhancing corporate responsibility, transparency, and governance in corporations. CEOs and CFOs are cautious and make sure they abide by the act's regulations, considering the severe fines that can be levied for deliberate data breaches (Hillier, McColgan & Tsekeris, 2022).[68]

The constant technological advancements impose a great challenge for regulators, but it is apparent that federal laws and regulations focused on corporate protection of data and operations against cybercrime are lagging. The newly proposed SEC regulation attempts to fill this gap.

Cyber threats and events increasingly cause costs to public companies and their investors, while there is substantial under-reporting of these issues in the public. Thus, the SEC adopted a rule on cybersecurity risk management, strategy, governance, and incident disclosure which was proposed in March 2022 and adopted in July 2023. The rule implements two major disclosure changes: (i) current ad hoc disclosure about material cybersecurity incidents, and (ii) periodic disclosure about board oversight and the role and expertise of management in identifying and mitigating cybersecurity risks.

The rule adds a new dedicated item (Item 1.05) to Form 8-K[69] labelled "Material Cybersecurity Incidents" and mandates disclosure within four business days after a firm determines that a cybersecurity incident is material. The following pieces of information need to be reported under Item 1.05: (i) when the event was detected and whether it is still problematic; (ii) a succinct explanation of the incident's nature and breadth; (iii) if any information was misappropriated, changed, accessed, or utilized for any other unlawful function; (iv) the incident's impact on the business operations; and (v) whether the business has addressed the incident or is still in the process of doing so. The occurrence of a material cybersecurity incident (as opposed to just any cybersecurity incident), triggers the company's disclosure responsibility under Item 1.05. The firm is required to "make a materiality determination about a cybersecurity event as soon as is reasonably practical after the discovery of the incident".[70] The

[66] In the field of financial infrastructure, the Commodity Futures Trading Commission Derivatives Clearing Organisations Regulation (CFTC) ensures that derivatives clearing businesses must create a comprehensive and effective information security program that encompasses a mandatory yearly compliance report to the board and CFTC.

[67] The maximum penalties for false certification are USD 1 million and 10 years of imprisonment, and wilful filing can lead to a fine of USD 5 million and 20 years in prison.

[68] While the Sarbanes-Oxley Act (SOX) does not explicitly refer to cybersecurity or data breaches, its requirements for internal controls over financial reporting (Sections 302 and 404) may indirectly apply when cyber incidents threaten the integrity of financial data or accounting systems. In such cases, companies may have disclosure obligations, especially under related SEC guidance.

[69] The comprehensive Form 8-K is designed to inform investors in U.S. public corporations of specific events that might be significant to shareholders or the SEC.

[70] See: https://www.sec.gov/files/rules/final/2023/33-11216.pdf.

rule also specifies that failure to timely file an Item 1.05 of Form 8-K would not adversely affect Form S-3[71] eligibility and (2) extend the limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Securities Exchange Act of 1934.[72] Tying the disclosure trigger to materiality gives companies the flexibility to accurately assess – difficult though this may be – the scope of an incident before the four-day disclosure clock starts to run.[73] To ensure that information security officials who are aware of the specifics and significance of an incident promptly communicate with officers in charge of disclosure decisions, companies will need to put in place robust procedures. The new rule also requires disclosure on any significant updates about previous incidents in annual and quarterly filings, i.e., on Forms 10-K and 10-Q.[74]

In addition to ad-hoc reporting, the new rule mandates that firms periodically report information on their cybersecurity risk management and strategy as part of its Form 10-K[75], under a new Item 106 of Regulation S-K.[76] More specifically, in the section "Risk management and strategy" firms must describe the processes that they use to identify, assess and manage the risks from cybersecurity incidents and how these risks affect the firm from the perspective of its business strategy, operations, and financials. In the section titled "Governance", firms must disclose how the board of directors oversees the risk of cybersecurity threats and how management assesses and manages these risks. In sum, the SEC's rule in 2023 aimed to tackle the issue of under-disclosure to provide more timely and more consistent information about cybersecurity risks.

### *3.7* Laws to Address Specific Industry Vulnerabilities

Industry-specific regulation exist to mitigate distinct vulnerabilities. Currently, specific rules in IT security apply to the financial sector, defence firms[77], healthcare industry, and infrastructure, where governmental agencies monitor cyber risk as a systemic hazard to the country. While many

[71] Form S-3 is a securities registration form that companies use to register securities with the SEC. Using Form S-3 allows eligible companies to register securities in a simplified and more streamlined process, as compared to other forms such as Form S-1. It also enables companies to use "shelf registration" which allows them to periodically sell securities from a pre-existing registration statement, instead of having to file a new registration statement for each securities offering.

[72] SEC Rule 10b-5, states that it is illegal for any person to defraud or deceive someone, including through the misrepresentation of material information, with respect to the sale or purchase of a security.

[73] Still, item 1.05 of the 8-K filing does not allow for a delay in disclosure during an investigation on materiality determination during a rapidly developing situation.

[74] An annual report called Form 10-K is mandated by the SEC and provides a detailed summary of a company's financial performance. Publicly traded companies are also required to file Form 10-Q, a quarterly report, with the SEC.

[75] See: https://corpgov.law.harvard.edu/2022/04/05/sec-proposes-rules-enhancing-cybersecurity-disclosures/.

[76] Regulation S-K is a disclosure framework established by the SEC that mandates public companies to provide investors and the public with detailed information about their business operations, financial condition, risk factors, management and executive compensation, and relationships with related parties. The purpose of Regulation S-K is to enable investors to make informed investment decisions. Companies must comply with the regulation's disclosure requirements when registering their securities with the SEC and filing various reports.

[77] For example, the Defence Federal Acquisition Regulation states that contractors of the DoD are required to ensure strict security to protect "covered defence information" on unclassified information systems (specific NIST standards must be followed to adhere to the regulation).

cybersecurity regulations in the U.S. target specific industries such as healthcare or finance, certain laws apply more broadly to address cross-sectoral vulnerabilities. One such law is the Computer Fraud and Abuse Act (CFAA), enacted in 1986 and codified at 18 U.S. Code § 1030, which remains a central legal instrument in the U.S. for combating cybercrime. It criminalises a broad range of activities involving unauthorised access to computers and data, including hacking, data theft, denial-of-service attacks, and the transmission of malicious code. The CFAA applies to both external attackers and insiders who exceed their authorised access and cause damage or steal information. Although its scope has been narrowed in recent jurisprudence (e.g. *Van Buren v. United States*, 2021), the law continues to serve as a foundation for the prosecution of cyber offences by the Department of Justice and is frequently used in combination with other federal statutes in both criminal and civil actions.

### *3.7.1 Infrastructure*

The Presidential Policy Directive for Critical Infrastructure Security and Resilience was established in February 2013. Three strategic imperatives were outlined in this policy: improve and clarify functional linkages across the federal government, facilitate efficient information interchange, and put in place a function for integration and analysis to help with planning and operations decisions. (Wagner, 2021) lists the many government agencies overseeing critical infrastructures in the U.S.:

- The Department of Homeland Security: chemical industry; commercial facilities, communications; critical manufacturing; dams; defence industrial base; emergency services; government facilities; information technology; nuclear reactors, materials, and waste; and transportation sectors.
- The Environmental Protection Agency: water and wastewater systems sector.
- The Department of Health and Human Services: healthcare and the public sector (Medicare and Medicaid, medical research, food and drug safety, and public health emergencies like pandemics).
- The Department of Agriculture and Department of Health and Human Services: food and agricultural sector.
- The Department of Treasury: financial services sector.
- The Department of Energy: energy sector.

### *3.7.2 Healthcare and Finance*

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) for healthcare and the Sarbanes Oxley (SOX, 2002) and Payment Card Industry - Data Security Standard (PCI-DSS, 2006) for the financial industry, are among the most well-known cybersecurity regulations in the Health and Finance industries (Neto, Madnick, de Paula, & Borges, 2020). In particular, the HIPPA Act established national standards to protect sensitive patient health information from being disclosed without the patient's permission or knowledge (Sales, 2013). The HIPPA also allows access rights to individuals' protected health information, such as the ability to inspect and receive a copy of medical records, ask

for corrections, and instruct a covered entity to send their protected health information in an electronic format to a different party (U.S. Department of Health and Human Services (HSS), 2022).

Even though businesses with weak cyber-defences in the financial services industry rarely face the civil lawsuits, the industry is subject to liability under the SOX Act as well as the Gramm-Leach-Bliley Act of 1999 (GLB Act) for data breaches (Sales, 2013). The regulation mandates that organisations create and maintain a thorough information security program with administrative, technical, and physical safeguards that are appropriate to its size and complexity, the nature and scope of its operations, and the sensitivity of any customer information at risk (Legal Information Institute, 2022a).

In addition to the SOX and GLB, all businesses that accept, process, store, or transmit credit card information are required to maintain a secure environment by the Payment Card Industry Data Security Standard (PCI-DSS). Major credit card firms including Visa, MasterCard, American Express, and Discover developed the standard to safeguard sensitive data and lower the possibility of credit card fraud. The PCI-DSS[78] mandates that organisations maintain secure networks, safeguard cardholder data, put in place strict access controls, frequently test, and monitor networks, and maintain an information security policy in order to protect cardholder data.[79]

Another important regulation in the financial sector is the Fair Credit Reporting Act (FCRA; 15 U.S. Code § 1681), which governs the collection, accuracy, and sharing of personal credit information. While not a cybersecurity law per se, the FCRA plays a key role in data privacy, as it grants individuals the right to access and correct their credit records, restricts unauthorised use of credit data, and imposes obligations on credit reporting agencies to ensure data is used fairly and transparently. This reflects a sector-specific approach to privacy, contrasting with more comprehensive frameworks like the GDPR in the EU.

In late 2024, the U.S. Department of Health and Human Services (HHS) issued a major update to the HIPAA Security Rule, reflecting the evolving cybersecurity landscape in the healthcare sector. The amendments introduce more granular and mandatory safeguards, including requirements for multi-factor authentication (MFA), encryption of electronic protected health information (ePHI) both in transit and at rest, and the implementation of continuous vulnerability management systems. Covered entities and their business associates must also conduct periodic, documented risk assessments and update their mitigation procedures accordingly.

These changes aim to address the increased attack surface created by the growing use of telehealth services, mobile health apps, and cloud-based storage for sensitive health data. In addition to updating the technical safeguards, the rule clarifies breach notification thresholds and expands the scope of enforcement actions undertaken by the Office for Civil Rights (OCR). The tiered penalty system remains in place, with fines of up to USD 1.5 million per violation category, depending on the nature and severity of non-compliance.

[78] See: https://www.pcisecuritystandards.org/, and
https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf
[79] The U.S. regulates electronic signatures through the Electronic Signatures in Global and National Trade Act (2000) and the Uniform Electronic Transactions Act (1999).

The 2024 update is part of a broader regulatory shift toward cybersecurity resilience and accountability in healthcare, a sector increasingly targeted by ransomware and data exfiltration attacks. It reflects HHS's intention to align HIPAA with emerging best practices and to signal that baseline compliance must now include proactive and adaptive security measures rather than static checklists (U.S. Department of Health and Human Services, 2024).Even if compliance controls do exist and vendor guidance is in place to enable businesses to secure their information technology and cyber environments, the numerous occurrences of information leaks reveal that enterprises have not been able to adapt effectively to use and manage the security of new (cloud) computing environments. To promote local businesses globally, regulatory bodies must make sure that the right compliance frameworks and laws are in place (Neto et al., 2020).

#### *3.7.3 Online Services and Children*

The Children's Online Privacy Protection Act (COPPA), enacted in 1998 and codified at 15 U.S. Code Chapter 91, is a key federal law regulating the online collection of personal information from children under the age of 13. It requires operators of websites and online services aimed at children, or those that knowingly collect data from children, to obtain verifiable parental consent before gathering, using, or sharing such information. COPPA also mandates clear privacy policies and gives parents the right to review and delete their child's personal data. Enforced by the Federal Trade Commission (FTC), COPPA has led to substantial penalties against major platforms for violations, highlighting its importance in protecting vulnerable user groups in the digital environment (U.S. Congress, 1998).

### 3.8 The Electronic Signatures in Global and National Commerce Act (ESIGN)

The Electronic Signatures in Global and National Commerce Act (ESIGN, 2000, 15 U.S. Code § 7001 et seq.) and the Uniform Electronic Transactions Act (UETA, 1999,15 U.S. Code §§ 7001-7031) are respectively a federal law and a regulation adopted by the states and provide a legal framework for electronic signatures and transactions. The ESIGN federal law establishes the legal equivalence of electronic signatures and electronic records with their paper counterparts in the context of transactions affecting interstate or foreign commerce. This means that electronic signatures and records are considered legally binding and enforceable in the same way as traditional signatures and paper records. UETA is a model law created by the National Conference of Commissioners on Uniform State Laws[80], which has been adopted by 47 states. UETA is similar to ESIGN in that it provides a legal framework for electronic transactions, including electronic signatures, records, and contracts. However, unlike ESIGN, UETA applies only to within-state transactions.

[80] The UETA model was developed by the Uniform Law Commission (ULC), a private organisation that proposes uniform laws for adoption by states, and serves as a guide for states that choose to adopt it.

Both ESIGN and UETA establish the requirements for a valid electronic signature, including the intent to sign, the association of the signature with the record, and the ability to authenticate the signature. They also provide guidelines for the use of electronic records in various contexts, including consumer transactions, government transactions, and legal proceedings. Overall, ESIGN and UETA have helped to facilitate the growth of electronic commerce by providing a legal framework for electronic signatures and transactions that is recognized and enforced across different jurisdictions.

### 3.9 Dealing with Transnational Data Security: The CLOUD Act (2018)

The Clarifying Lawful Overseas Use of Data Act (CLOUD – House of Representatives HR 4943) was passed in 2018 to streamline the conditions and processes for both international and domestic investigators seeking access to electronic (personal and private) data kept by service providers. Authorities from all over the world use data to investigate major crimes, including terrorism, violent crime, child sex exploitation, and cybercrime. The number of requests for mutual legal aid that ask for electronic evidence from the U.S. has substantially increased in recent years, especially as foreign organisations need access to data kept by a company with headquarters in the U.S. The CLOUD Act modernizes the legal frameworks and protocols to address the revolution in electronic communications and advancements in the system configuration practices of major international technology businesses. To fight serious crime and terrorism, the act allows foreign allies with strong privacy and civil liberties protections to engage in executive agreements with the U.S. to acquire electronic evidence. The CLOUD Act thus marks a shift in thinking: an effective, privacy-protective approach to public safety by facilitating quick access to electronic data within the bounds of pre-existing legal frameworks. This strategy upholds high standards of privacy and civil liberties protection while making the U.S. and its allies safer.[81]

As it permits foreign governments with weaker privacy protections to access U.S. residents' data without proper monitoring or due process, critics claim that the Act violates the right to privacy. The Act has also drawn criticism for possibly enabling foreign governments to utilize the information for human rights violations or other forms of political repression. A number of civil liberties groups and privacy advocates have demanded that the CLOUD Act be changed or repealed.[82]

### 3.10 Legal Work in Progress

#### *3.10.1 The Quantum Computing Cybersecurity Preparedness Act*

Introduced in late 2023 and signed into law as H.R.7535, the Quantum Computing Cybersecurity Preparedness Act requires the National Institute of Standards and Technology (NIST) to

[81] See: https://www.justice.gov/criminal-oia/page/file/1153466/download.
[82] See: https://www.aclu.org/news/privacy-technology/cloud-act-dangerous-piece-legislation.

develop and promote standards for safeguarding federal information systems against the risks posed by quantum computing. In particular, the Act emphasises the need to transition from classical to post-quantum cryptography (PQC), which is resistant to the decryption capabilities of quantum machines. It directs NIST to coordinate with agencies such as the Department of Defense (DoD) and the Department of Homeland Security (DHS) to identify vulnerabilities in quantum supply chains and ensure cryptographic agility in critical federal systems.

The legislation reflects growing concern that nation-states or adversaries may harvest encrypted data today with the intention of decrypting it in the future once quantum capabilities mature ("harvest now, decrypt later" attacks). By establishing a strategic roadmap for quantum-resilient cybersecurity, the Act serves as an early legislative response to one of the most disruptive emerging technologies. While the Act primarily targets federal agencies, its guidance is expected to influence best practices across critical infrastructure sectors and public-private partnerships in cybersecurity (U.S. Congress, 2023).

#### *3.10.2 Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)*

Enacted in March 2022, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) establishes a binding federal incident-reporting regime aimed at enhancing national cyber resilience. Under the Act, entities operating in designated critical infrastructure sectors, such as energy, communications, water, and healthcare, are required to report covered cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours, and any ransomware payments within 24 hours.

CISA is tasked with analysing submitted reports, disseminating anonymised threat intelligence to stakeholders, and developing detailed implementation rules. These will be formalised following the notice of proposed rulemaking (NPRM) process. CIRCIA reflects a shift from voluntary to mandated incident disclosure at the federal level, with the goal of improving real-time situational awareness, facilitating cross-sectoral coordination, and strengthening the United States' response capacity to cyber threats (CISA, 2024).

#### *3.10.3 NY DFS Cybersecurity Regulation*

The New York Department of Financial Services (NY DFS) Cybersecurity Regulation (23 NYCRR Part 500) was first enacted on March 1, 2017 and received its first amendment in April 2020. The most substantial update, known as the Second Amendment, was adopted on November 1, 2023, with a staggered implementation timeline extending into 2025. The updated regulation requires New York–chartered financial institutions to maintain a comprehensive cybersecurity programme, including multi-factor authentication, encryption of non-public information, annual risk assessments, incident response planning, and business continuity measures. The 2023–2024 amendments introduce more stringent controls: enhanced board and senior-level governance responsibilities (including an expanded

role for the CISO), mandatory independent cybersecurity audits, annual penetration testing, and more robust vulnerability management protocols. Non-compliance may result in civil penalties or even licence restrictions imposed by the DFS. As one of the most prescriptive and actively enforced cybersecurity regimes in the U.S., the NY DFS regulation serves as a benchmark for financial sector oversight and has shaped broader regulatory discourse across jurisdictions (New York State Department of Financial Services, 2023).

**4. Comparison between EU and U.S. Regulations and Conclusion**

This paper summarizes and compares the regulation of data privacy and cybersecurity between the EU and the U.S. While Europe is heavily focused on privacy and data exchange (GDPR), the U.S. lacks such a federal regulation, exhibiting a patchwork of cybersecurity regulations that vary substantially by state and by sector. However, the U.S. does have federal legislation, such as the Cybersecurity Information Sharing Act (CISA) and the Computer Fraud and Abuse Act (CFAA), that can apply to specific areas of cybersecurity. The GDPR applies extraterritorially to any organisation that processes the personal data of EU residents, regardless of where the organisation is based. In contrast, most U.S. regulations apply to organisations based in the U.S. or operating within regulated sectors, and are generally designed to protect U.S. citizens or residents.Moreover, the GDPR has a wider scope, covering areas such as data protection impact assessments, data breach notification, and incorporating privacy aspects into products, services, and systems by design. Particularly, there is a fundamental difference in the approach to data exchange: GDPR mandates obtaining an explicit consent from individuals before collecting and processing their personal data, and these individuals have the right to withdraw their consent at any time. In contrast, there is no federal law in the U.S requiring explicit consent; instead, privacy laws focus more on transparency and on individuals' right to access and correct their personal data. The GDPR imposes fines for non-compliance (up to EUR 20 million or 4% of an organisation's global revenue, whichever is higher), while in the U.S. penalties are often lower and vary by regulation although civil and criminal penalties can be imposed (through e.g., the CFAA and HIPAA Acts, respectively addressing computer fraud and health insurance).

For shareholders and stakeholders in the U.S., it is difficult to monitor the right level of data privacy protection applied by organisations, as the delegation to state-level legislation leads to fragmentation, opacity, and voids (Nicola & Pollicino, 2020). Consequently, there is no unified framework with definitions of a (material) data breach, reporting thresholds, enforcement responsibilities, penalties for violations, application scope (e.g., citizens in other states subject to data issues by a corporation in a home state) etc.

This regulatory fragmentation also creates significant compliance complexity for organisations operating across multiple states or sectors, as they must navigate inconsistent standards, overlapping reporting obligations, and different enforcement practices.

The EU has developed strict rules for government surveillance and data retention (by means of the GDPR and other directives). The U.S. has implemented the Foreign Intelligence Surveillance Act (FISA), which allows for the collection of intelligence information for national security purposes.

Finally, the GDPR requires organisations to notify individuals and authorities within 72 hours of a data breach, whereas the U.S. has various state and federal data breach notification laws, with some states requiring notification within 30 days of discovery. However, both the EU and the U.S. suffer from limitations in terms of incident disclosure.

Both the EU and the U.S. have established laws to address cybersecurity concerns, calling for the adoption of industry best practices to enhance system resilience. The EU introduced the NIS (Network and Information Systems) Directive in 2016 and passed the Cybersecurity Act (EU 2019/881), which strengthened the mandate of ENISA (the European Union Agency for Cybersecurity) and established an EU-wide cybersecurity certification framework, while the U.S. launched the NIST Cybersecurity. Framework in 2014 as a voluntary set of standards to help organisations assess and manage cyber risks.

While the EU and the U.S. agree on the importance of certification and baseline cybersecurity requirements, they pursue distinct approaches. EU member states require all organisations to follow the NIS Directive for the best safeguards, yet the adoption of the NIST Framework in the U.S. is voluntary.

The mandatory disclosure regulation of data breaches and privacy violations are still insufficient in both Europe and the U.S. In Europe, information on data and privacy breach cases is not centrally collected, and the existing mandatory disclosure regulation in the U.S. (at the state level) leads to identification of only a small fraction of the actual data breach events. Disclosure of cyber incidents that have not (yet) resulted in known data losses is also not centrally gathered in Europe and only sparsely, if at all, across industries in the U.S. The absence of standardised, centralised disclosure frameworks in both jurisdictions limits the ability of public authorities, researchers, and market participants to assess systemic cyber risks. As a result, market discipline remains weak: investors, suppliers, and consumers cannot reliably evaluate firms' cyber exposure or security posture.

This paper also examines the regulations in the realm of fighting cybercrime through the implementation of minimum cybersecurity levels, and demonstrates how complex, heterogenous, and incomplete the regulatory landscape is. Remarkably, there is no encompassing up-to-date federal law regulating cybersecurity in the U.S. as this regulation was delegated to the individual states who are responsible for standard setting and compliance. Furthermore, cybersecurity regulation has been developed for specific industries and critical infrastructure. This has resulted in a proliferation of enforcement agencies with heterogeneous standards, reporting requirements, and penalties. The current (criminal, civil, and securities) laws governing cyber conflicts are insufficient to address (and penalize) cybersecurity deficiencies and the underinvestment in cyber protection by public and private businesses as well as public organisations. In the presence of negative externalities created by cyber risks, the social value of investments in cybersecurity is likely to exceed the private value from the perspective of the individual organisation, further aggravating the underinvestment problem in cybersecurity.

Mandatory disclosure frameworks might encourage cybersecurity investments, as they enable monitoring by a wide range of stakeholders, including equity and debt investors, suppliers and customers, citizens, employees, communities, non-governmental institutions, law enforcement agencies, etc. While in the U.S. the SEC currently explores a proposal to standardize the ad-hoc disclosure of cyber incidents and cybersecurity, disclosure is even less stringent in the EU. Most European countries do not maintain a centralised public disclosure platform for cybersecurity incidents that is easily accessible to a wide range of public stakeholders. The European Data Protection Board (EDPB)[83] which brings together the different supervisory authorities in the EU, might be the right institute to take the lead in the future. Nevertheless, only the supervisory authorities i.e., the country-level authorities hold incident data, and no aggregation at the European level is available, which undermines an effective transnational strategy.

Both the EU and the U.S. have made important advances in addressing cybersecurity and data privacy, but their regulatory frameworks remain fragmented, reactive, and incomplete. The EU has a comparative advantage in legal coherence and scope, while the U.S. benefits from sector-specific technical depth and public-private coordination. Yet neither system fully addresses the economic incentives behind underinvestment in cybersecurity, nor do they provide the kind of consistent, centralised, and transparent cyber incident reporting infrastructure that would enable meaningful oversight. Closing these gaps, whether through regulatory convergence, stronger enforcement mandates, or institutional innovation, is essential to building resilient digital economies in the face of rapidly evolving threats.

[83] The European Data Protection Supervisor (EDPS) and the EC ensure the consistent application of the EU data protection framework. In particular, the EDPB has the competence to (i) provide general guidance (including guidelines, opinions, recommendations, and best practices) on data protection laws, specifically regarding the GDPR, (ii) advise the EC on any issue related to protection of personal data and new proposed legislation in the EU, and (iii) adopt consistent decisions and opinions in cross-border data protection cases.

**References**


Boehm, F. (2015). *A comparison between U.S. and EU data protection legislation for law enforcement purposes*. Strasbourg, France: European Parliament. Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%2953 6459_EN.pdf

Cochran, Z., Z. Davis & E. Morgan. (2022, April 5). SEC Proposes Rules Enhancing Cybersecurity Disclosures. Harvard Law School Forum on Corporate Governance. https://corpgov.law.harvard.edu/2022/04/05/sec-proposes-rules-enhancing-cybersecurity-disclosures/

Cole, M. & S. Schmitz. (2019). The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape (December 31, 2019). University of Luxembourg Law Working Paper No. 2019-017.

Congress. (2017). H.R.3806 - Personal Data Notification and Protection Act of 2017; from www.congress.gov: https://www.congress.gov/bill/115th-congress/house-bill/3806/text

Congress. (2022). H.R.4081 - Consumer Privacy Protection Act of 2017. Retrieved from www.congress.gov: https://www.congress.gov/bill/115th-congress/house-bill/4081#:~:text=This%20bill%20amends%20the%20federal,least%20%241%2C000%20to%20any%20individual

Cybersecurity Ventures. (2025). Cybercrime To Cost The World $12.2 Trillion Annually By 2031.

Cybersecurity and Infrastructure Security Agency. (2024). Cyber Incident Reporting for Critical Infrastructure Act of 2022 – Notice of Proposed Rulemaking. Federal Register. Retrieved from https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

Crime Magazine, May 28, 2025. Retrieved from: https://cybersecurityventures.com/official-cybercrime-report-2025/

Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view, Computer Law & Security Review 34(3), 477-495, ISSN 0267-3649, (https://www.sciencedirect.com/science/article/pii/S0267364917303953)

Department of Homeland Security. (2022). Cybersecurity. Retrieved from www.dhs.gov/: https://www.dhs.gov/topics/cybersecurity

ECB. (2022a). Sanctions. Retrieved from European Central Bank - Banking Supervision: https://www.bankingsupervision.europa.eu/banking/tasks/sanctions/html/index.en.html

ECB. (2022b). What is TIBER-EU? Retrieved from https://www.ecb.europa.eu/:https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html#:~:text=TIBER%2DEU%20is%20the%20European,carrying%20out%20a%20controlled%20cyberattack

ENISA. (2020). NIS Directive. Retrieved from https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

ENISA. (2021). CSIRT Capabilities in Healthcare Sector. Retrieved from www.enisa.europa.eu: https://www.enisa.europa.eu/publications/csirt-capabilities-in-healthcare-sector

ENISA. (2022a). EU Cybersecurity Initiatives in the Finance Sector. Retrieved from https://www.enisa.europa.eu: https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector

ENISA. (2022b). Supporting the implementation of Union policy and law regarding cybersecurity. Retrieved from https://www.enisa.europa.eu: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

ENISA. (2023). NIS 2 Directive – The new EU cybersecurity rules. Retrieved from https://www.enisa.europa.eu: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis2-directive

European Commission. (2019). Directive (EU) 2019/1024 on Open Data and the Re-use of Public Sector Information (OD-PSI Directive). Retrieved from eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024

European Commission. (2022). Digital Markets Act (DMA), Regulation (EU) 2022/1925. Retrieved from eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925

European Commission. (2023). *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows*. Retrieved from ec.europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

European Commission. (2024). Cyber Resilience Act: Regulation (EU) 2024/2847 on cybersecurity requirements for products with digital elements. Retrieved from eur-lex.europa.eu: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

European Parliament & Council. (2016). 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 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union, L 333, 27.12.2022. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554

European Commission. (2020). Commission Staf Working Document, Impact Assessment Report. Retrieved from digital-strategy.ec.europa.eu:https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020SC0345&rid=6

European Commission. (2022a). ec.europa.eu. Retrieved from EU Member States notifications to the European Commission under the GDPR: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en

European Commission. (2022b). NIS Directive. Retrieved from digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/policies/nis-directive

European Commission. (2022c). The EU Cybersecurity Act. Retrieved from digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

European Commission. (2022d). NIS Cooperation Group. Retrieved from https://digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

European Commission. (2022e). Cyber Defence: EU boosts action against cyber threats. Retrieved from ec.europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642

European Commission. (2022f). The Digital Services Act package. Retrieved from digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

European Commission. (2022g). Critical Infrastructure: Commission accelerates work to build up European resilience. Retrieved from ec.europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238

European Commission. (2022h). EU Cyber Resilience Act. Retrieved from digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Commission. (2022i). European Data Governance Act. Retrieved from digital-strategy.ec.europa.eu/en/: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

European Commission. (2022j). A European approach to artificial intelligence. Retrieved from digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

European Commission (2022k). Data Act: Commission proposes measures for a fair and innovative data economy. Retrieved from https://ec.europa.eu/commission/presscorner: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

European Commission. (2023a). eIDAS Regulation. Retrieved from digital-strategy: https://digital-strategy.ec.europa.eu/

European Commission. (2023b). Free Flow of Non-Personal Data. Retrieved from digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/policies/non-personal-data

European Commission. (2024). Regulation (EU) 2024/482 establishing the European Common Criteria-based cybersecurity certification scheme (EUCC). Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R0482

European Commission. (2025). Digital Networks Act: Public consultation on future EU digital infrastructure rules. Retrieved from Digital Strategy EU: https://digital-strategy.ec.europa.eu/en/news/commission-gathers-feedback-upcoming-digital-networks-act

European Council. (2022). Data protection in law enforcement. Retrieved from https://www.consilium.europa.eu: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-law-enforcement/

European Energy Information Sharing & Analysis Centre. (2022). European Energy Information Sharing & Analysis Centre. Retrieved from ee-isac.eu/: https://www.ee-isac.eu/

European Parliament. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Retrieved from EUR-Lex: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

Federal Trade Commission. (2024, December 13). Lenses of security: Preventing and mitigating digital security risks through data management, software development, and product design for humans. Office of Technology & Division of Privacy and Identity Protection. Retrieved from https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/lenses-security-preventing-mitigating-digital-security-risks-through-data-management-software

Ferraro, G.C., 2020. Data breaches should not be a virtual certainty: adopting the NIST standard for cybernegligence. *Washburn Law Journal 59*, 489-518.

Garrison, C. & C. Hamilton. (2019). A comparative analysis of the EU GDPR to the U.S.'s breach notifications. Information & Communications Technology Law. 28. 1-16. 10.1080/13600834.2019.1571473.

Ghosh, I. (2019). This is the crippling cost of cybercrime on corporations. Retrieved from weforum.org: https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/

Hillier, D., P. McColgan, & A. Tsekeris, (2022). How did the Sarbanes–Oxley Act affect managerial incentives? Evidence from corporate acquisitions. Springer Nature Switzerland AG. Review of Quantitative Finance and Accounting 58, 1395–1450. https://doi.org/10.1007/s11156-021-01028-6

Information Commissioner's Office. (2022). Overview – Data Protection and the EU. Retrieved from ico.org.uk: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/#:~:text=in%20the%20EEA

Kosseff, J. (2016). Positive cybersecurity law: Creating a consistent and incentive-based system. *Chapman Law Review 19*, 401-420.

Legal Information Institute. (2022a). 16 CFR § 314.3 - Standards for safeguarding customer information. Retrieved from: https://www.law.cornell.edu/: https://www.law.cornell.edu/cfr/text/16/314.3

Legal Information Institute. (2022b). Preemption. Retrieved from https://www.law.cornell.edu: https://www.law.cornell.edu/wex/preemption

Lunn, B. (2014). Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine. Journal of Law & Cyber Warfare, 4(1), 109–137.

Michels, J. D. & I. Walden. (2018). How Safe is Safe Enough? Improving Cybersecurity in Europe's Critical Infrastructure Under the NIS Directive. Queen Mary School of Law Legal Studies Research Paper No. 291/2018, Available at SSRN: https://ssrn.com/abstract=3297470

Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Retrieved from cybersecurityventures.com: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

NCSL (2022). Security Breach Notification Laws. Retrieved from https://www.ncsl.org/: https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws

Neto, N., Madnick, S., de Paula, M. & M. Borges. (2020). A case study of the capital one data breach. Working Paper MIT. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542567

New York State Department of Financial Services. (2023, November 1). Amendment to Cybersecurity Regulation – 23 NYCRR 500. Retrieved from https://www.dfs.ny.gov/industry_guidance/cybersecurity

Nicola, F.G. & O. Pollicino. (2020). The Balkanization of Data Privacy Regulation. West Virginia Law Review 123, 61-115.

Rustad, M. & T. Koenig. (2019). Towards a global data privacy standard. *Florida Law Review 71*, 365-450.

Sales, N. A. (2013) Regulating Cyber-Security (April 5, 2012). Northwestern University Law Review, Vol. 107, No. 4, pp. 1503-1568.

Saqib, N., Germanos, V., Zeng, W. & L. Maglaras (2020). Mapping of the Security Requirements of GDPR and NIS. *EAI Endorsed Transactions on Security and Safety*, *7*(24). https://eudl.eu/doi/10.4108/eai.30-6-2020.166283

Schaefer, H-B. & F. Mueller-Langer. (2008). Strict Liability Versus Negligence. Working Paper, Universität Hamburg - Fachbereich Rechtswissenschaf. Available at SSRN: https://ssrn.com/abstract=2062787 or http://dx.doi.org/10.2139/ssrn.2062787

Sekaran, S. (2022). GDPR Simplified: Distilling Its Significance on Infrastructure. Retrieved from https://www.cohesity.com: https://www.cohesity.com/blogs/gdpr-simplified-distilling-its-significance-on-infrastructure/

Shackelford, S. J., A Proia, B. Martell, & A. Craig. (2015). Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. Texas International Law Journal 50, 305.

Schmitz-Berndt, S. & F. Anheier. 2021. Synergies in Cybersecurity Incident Reporting-The NIS Cooperation Group Publication 04/20 in Context. *European Data Protection Law Review 7*, 101-107.

Schmitz-Berndt, S. & M. Cole. 2022. Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act. *Applied Cybersecurity & Internet Governance 1,*1-17.

Trautman, . J. & P. Ormerod. (2017), Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach. American University Law Review 66, 1231.

U.S. Congress. (1986). Computer Fraud and Abuse Act (CFAA), 18 U.S. Code § 1030. Retrieved from law.cornell.edu: https://www.law.cornell.edu/uscode/text/18/1030

U.S. Congress. (1998). Children's Online Privacy Protection Act (COPPA), 15 U.S. Code Chapter 91. Retrieved from law.cornell.edu: https://www.law.cornell.edu/uscode/text/15/chapter-91

U.S. Congress. (2015). Cybersecurity Information Sharing Act (CISA), Title I of the Cybersecurity Act of 2015. Retrieved from congress.gov: https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf

U.S. Congress. (2022). *Quantum Computing Cybersecurity Preparedness Act, H.R. 7535* (Pub. L. No. 117-xxx). Enacted December 21, 2022. Retrieved from Congress.gov: https://www.congress.gov/bill/117th-congress/house-bill/7535

U.S. Department of Health and Human Services, Office for Civil Rights. (2024, December 27). HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen the Cybersecurity of electronic protected health information. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html

U.S. Department of Labor. (2022). Guidance on the Protection of Personal Identifiable Information. Retrieved from https://www.dol.gov: https://www.dol.gov/general/ppii

Wagner, P. (2021, March 26). Critical Infrastructure Security. Working Paper. SSRN. https://doi.org/10.2139/ssrn.3762693

Woods, A.K. (2018). Litigating data sovereignty. Yale Law Journal 128, 328-406.

**Figure 1. Count of Cyber Incidents Per Incident Type**

*This figure shows the distribution (count of incidents) of the main incident types for 21,714 incidents over the period 2005-2023 for U.S. listed firms.* Source: Zywave.

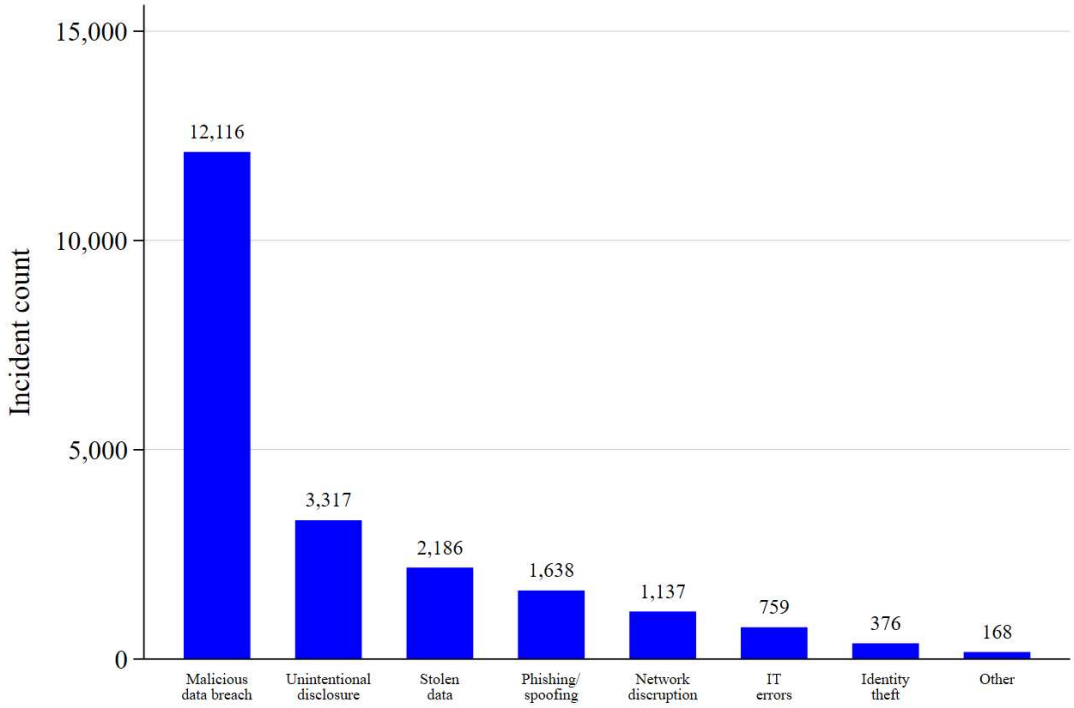


**Figure 2. Records Exposed by Perpetrator Type**

*This figure provides a breakdown for perpetrator type as per binned records exposed over the period 2005-2023 for U.S. listed firms. Data available for 16,409 incidents*. Source: Zywave.

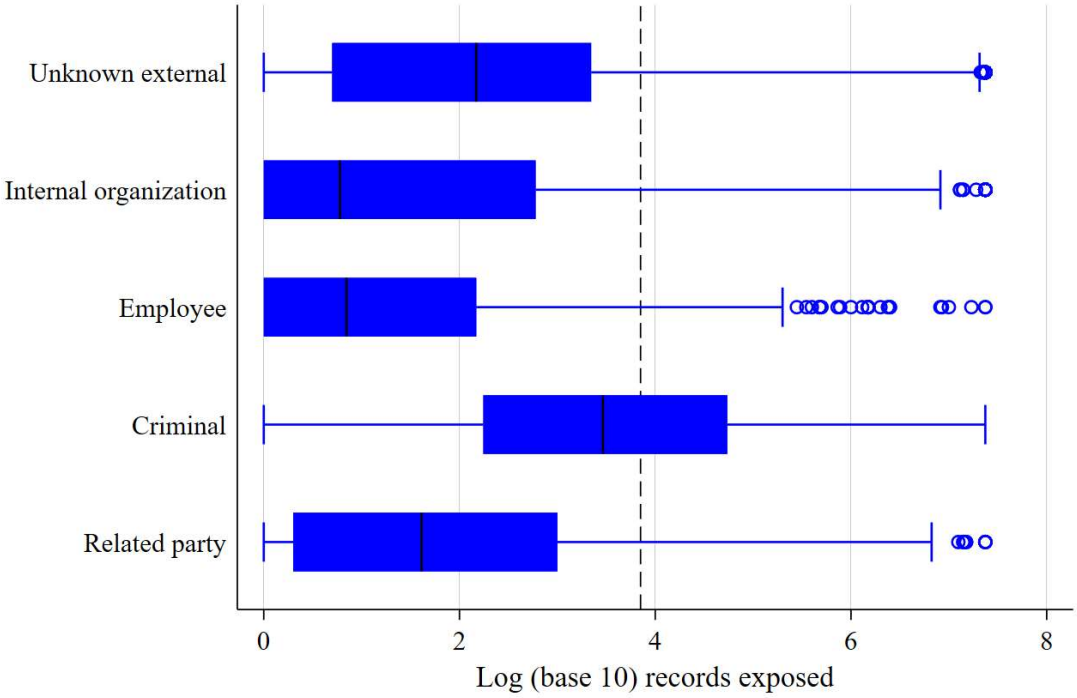
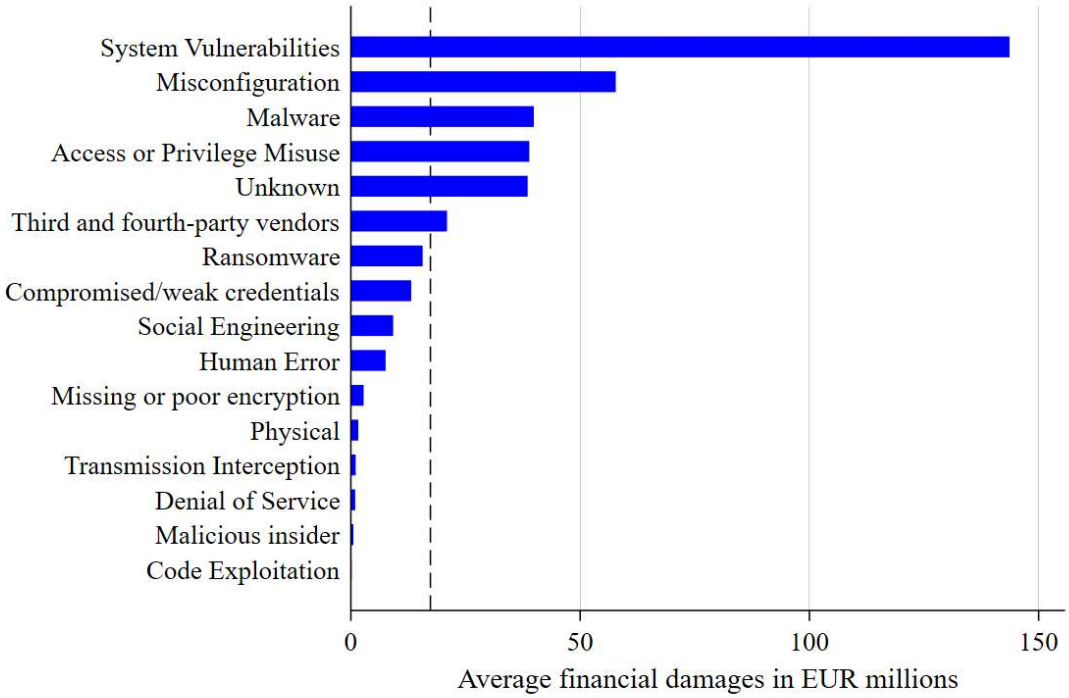


**Figure 3. Average Financial Damage Per Attack Vector**

*This figure provides a breakdown of average financial loss per attack vector over the period 2005-2023 for U.S. listed firms. Attack vector is the path or means by which the perpetrator gained access to data, a server.* Source: Zywave.



## Appendix 1: Glossary

| | |
|---|---|
| AI | Artificial Intelligence |
| ANSSI | French Network and Information Security Agency |
| B2B | Business-to-Business |
| B2G | Business-to-Government |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| CFAA | Computer Fraud and Abuse Act |
| CFR | Code of Federal Regulations |
| CFTC | Commodity Futures Trading Commission Derivatives Clearing Organisations |
| CISA(1) | Cybersecurity and Infrastructure Security Agency |
| CISA(2) | Cybersecurity Information Sharing Act |
| CLOUD | Clarifying Lawful Overseas Use of Data Act |
| CPMI | Committee on Payments and Market Infrastructures |
| CPPA | Privacy Protection Act of 2017 |
| CRA | Cyber Resilience Act |
| CROE | Cyber Resilience Oversight Expectations |
| CSAs | Concerned Supervisory Authorities |
| CSF | Cybersecurity Framework |
| CSIRTs | Computer Security Incident Response Teams |
| DA | Data Act |
| DGA | Data Governance Act |
| DHS | U.S. Department of Homeland Security |
| DoD | Department of Defence (U.S.) |
| DoJ | Department of Justice (U.S.) |
| DORA | Digital Operational Resilience Act |
| DPAs | Data Protection Agencies |
| DPC | Data Protection Commission (Ireland) |
| DSCs | Digital Services Coordinators |
| DSPs | Data Service Providers |
| EBA | European Banking Authority |
| EC | European Commission |
| ECC | European Cybersecurity Competence Centre |
| ECB | European Central Bank |
| ECPA | Electronic Communications Privacy Act |
| EDPB | European Data Protection Board |
| EDPS | European Data Protection Supervisor |
| EDTIB | European Defence Technological Industrial Base |
| EEA | European Economic Area |
| EE-ISAC | European Energy Information Sharing & Analysis Centre |
| eIDAS | Electronic Identification, Authentication and trust Services |
| EIOPA | European Insurance and Occupational Pensions Authority |
| ENISA | European Union Agency for Cybersecurity |
| EP | European Parliament |
| ESIGN | Electronic Signatures in Global and National Commerce Act |
| ESMA | European Securities and Markets Authority |
| FCRA | Fair Credit Reporting Act |
| FDA | Food and Drug Administration |
| FINRA | Financial Industry Regulatory Authority |
| FinTech | Financial Technology |
| FISA | Foreign Intelligence Surveillance Act |
| FMIs | Financial Market Infrastructures |
| FOIS | German Federal Office for Information Security |
| FTC Act | Federal Trade Commission Act |
| GDPR | General Data Protection Regulation |
| GLBA | Gramm-Leach-Bliley Act |
| H.R. | House of Representatives |
| HHS | Health and Human Services |
| HIPAA | Health Insurance Portability and Accountability Act |
| IAPP | International Association of Privacy Professionals |
| ICTs | Information and Communications Technology |
| IOSCO | International Organisation of Securities Commissions |

| | |
|---|---|
| IoT | Internet of Things |
| IRC | Incident Response Capabilities |
| IT | Information Technology |
| MiFID | Markets in Financial Instruments Directive |
| NCAs | National Supervisory Authorities |
| NIS | Network and Information Systems Directive |
| NIS2 | Network and Information Systems Directive 2 |
| NISCG | Network and Information Systems Collaboration Group |
| NIST Framework | National Institute of Standards and Technology Framework |
| NRAs | National Regulatory Authorities |
| OCR | Office for Civil Rights |
| OES | Operators of Essential Services |
| OMP | Office of Personnel Management |
| PCI-DSS | Payment Card Industry - Data Security Standard |
| PDNPA | Personal Data Notification & Protection Act |
| PII | Personally Identifiable Information |
| PSD2 | Revised Payment Services Directive |
| SCA | Stored Communications Act |
| SEC | Securities and Exchange Commission |
| SMEs | Small and medium-sized enterprises |
| SOCs | Security Operations Centres |
| SOX | Sarbanes-Oxley Act |
| TIBER-EU | Threat Intelligence-Based Ethical Red-Teaming |
| UETA | Uniform Electronic Transactions Act |
| VLOPs | Very large online platforms |
| VLOSEs | Very large online search engines |

**Appendix 2: Overview of the regulation on data security and cyber protection in the U.S. and the EU.**
This table offers an overview of the data security and cyber protection regulations in the U.S. (Panel A) and Europe (Panel B). The most important regulations in the context of cybersecurity and data breach are highlighted in bold italics.

## Panel A: U.S. Regulation

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| ***Federal Trade Commission Act (FTCA) §5, 15 U.S. Code § 45*** | ***1914*** | ***Most commercial entities in the U.S., excluding banks, federal credit unions, and common carriers*** | ***Natural person*** | ***Federal Trade Commission*** | ***Civil penalty of not more than USD 10k for each violation*** | ***Requires firms to implement all "reasonable and necessary" security procedures relating to data and cybersecurity. For businesses required to abide by Gramm-Leach-Bliley Act: FTC has issued Safeguards Rule (16 CFR 314). The Safeguards Rule, issued under the Gramm-Leach-Bliley Act, complements the FTC's enforcement authority under FTCA with concrete cybersecurity requirements for financial institutions.*** | ***Mandatory protection levels and minimum technical standards*** |
| Securities Act of 1933 | 1933 | Publicly listed firms | Natural and legal person (stock investors) | SEC | Section 24 provides for fines not exceeding USD 10k and prison term not exceeding 5 years. | Ensures more transparency in fin. Statements of corporations so investors can make informed investment decisions; establishes laws against misrepresentation and fraudulent activities in securities markets. | Data breach notification and fines |
| Fair Credit Reporting Act (FCRA) | 1970 | Credit reporting agencies and entities using credit data | Natural person | U.S. Federal Trade Commission (FTC) and Consumer Financial | Civil penalties; individual and class action liability; fines vary by case | Regulates the collection, accuracy, and use of personal credit information; provides individuals with rights to access and dispute their data | Sectoral privacy regulation (financial data) |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| | | | | Protection Bureau (CFPB) | | | |
| Federal Privacy Act | 1974 | Federal Agencies | Natural person | Self-enforced by each federal agency; oversight by the Office of Management and Budget (OMB); judicial enforcement via federal courts | Actual damages or USD 1,000 (the higher amount applies) | Controls how personally identifiable information about people is gathered, stored, used, and shared by federal agencies who operate records systems. All U.S. gov. agencies are prohibited from disclosing any records from a system of records to anybody or another agency without making a written request to the person to whom the record relates and after prior written consent of that individual. | Data breach notification and fines |
| ***Electronic Communications Privacy Act (ECPA) and Stored Communications Act (SCA) 18 U.S. Code Ch. 119 and 18 U.S. Code Ch. 121*** | ***1986*** | ***Natural or legal person*** | ***Natural person*** | ***U.S. Dpt of Justice*** | ***Fines up to USD 250k. Criminal sanctions are provided by the Acts, which may be used to imprison malicious hackers.*** | ***Restricts unwarranted monitoring, prohibits unauthorized use, disclosure, or access to any wire, oral, or electronic communication.*** | ***Data breach notification and fines*** |
| ***Computer Fraud and Abuse Act (CFAA)*** | ***1986 (amended multiple times, latest in 2008)*** | ***Any person or entity accessing protected computers without or in excess of authorization*** | ***Natural and legal person (victim of cybercrime)*** | ***U.S. Department of Justice*** | ***Criminal penalties: fines and imprisonment (up to 10 years for first offence; 20 years for repeat violations)*** | ***Prohibits unauthorised access to computers, data theft, and intentional damage to computer systems*** | ***Criminal cybercrime enforcement framework*** |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| Children's Online Privacy Protection (COPPA) Act, 15 U.S. Code Ch. 91, 16 CFR Part 312 | 1998 | Websites and online services aimed at children under 13. Also applies if website's creator knows for sure that young users are accessing the site. | Natural person | Federal Trade Commission | Civil penalties of up to $51,744 per violation, adjusted for inflation by FTC; higher cumulative fines possible in enforcement settlements. | Offers appropriate safeguards for privacy, security, and integrity of personal data acquire from children. Provides parents reasonable way to assess the personal data collected about their children and give option to reject its continued use or upkeep. A child cannot be required to disclose information in order to participate in a game, receive a prize, or engage in another activity. | Data breach notification and fines |
| ***Gramm-Leach-Bliley Act (GLBA), 5 U.S. Code Subchapter I*** | ***1999*** | ***Banks, insurance companies, securities firms, non-bank mortgage lenders, auto dealers offering financing, tax preparers, and other financial institutions subject to federal regulation*** | ***Natural person*** | ***Federal Trade Commission*** | ***Fines of more than USD 1 m.*** | ***Requires entities to "develop, implement, and maintain comprehensive information security program written in one or more readily accessible parts and contains administrative, technical, and physical safeguards appropriate to size and complexity, nature and scope of activities, and sensitivity of any customer information at issue."*** | ***Mandatory protection levels and minimum technical standards*** |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| ***Health Insurance Portability and Accountability Act (HIPAA) Act (45 CFR Part 160, and Part 164 )*** | ***Dec.28, 2000, and adopted modifications of Rule on Aug.14, 2002. First enacted in 1996.*** | ***Healthcare providers, health insurance plans (including Medicare/Medicaid), healthcare clearinghouses, and business partners handling protected health information*** | ***Natural person*** | ***HHS Office for Civil Rights*** | ***Severity of breach, organisation's efforts to secure info, and kind and breadth of infraction determine fine related to privacy breach. Aggregate penalties in 2018: USD 28 m.*** | ***Creates national standards to protect sensitive patient health information from being disclosed without patient's consent or knowledge.*** | ***Data breach notification and fines*** |
| ***SEC Regulation on Privacy of Consumer Financial Information and Safeguarding Personal Information (S-P), 17 CFR Part 248, Subpart A*** | ***2000*** | ***Publicly listed firms*** | ***Shareholder, Natural person*** | ***SEC and Financial Industry Regulatory Authority (FINRA)*** | ***Civil penalties can be USD 1,098,190 or triple the profit (whatever is larger).*** | ***Requires entities to create written procedures to preserve client records and guard against unauthorized access.*** | ***Data breach notification and fines*** |
| Homeland Security Act of 2002 | 2002 | Natural or legal person | Natural or legal person | Department of Homeland Security | Criminal and statutory penalties (section 1030 of title 18, U.S. Code: USD 10k or twice value obtained by offense) | Prevents and responds to natural and man-made disasters. Monitor border security, port of entry (also online), and cyberterrorism. | Data breach notification and fines |
| ***Sarbanes-Oxley (SOX), 15 U.S. Code Chapter 98*** | ***2002*** | ***Publicly listed firm*** | ***Shareholder*** | ***SEC*** | ***Max. penalty for false certification is USD 1m. and 10 years of imprisonment. Wilful filing can lead to fine of USD 5 m. and 20 years in prison.*** | ***Requires publicly listed firms under SOX to make cybersecurity certifications public.*** | ***Mandatory protection levels and min. technical standards*** |
| ***Regulations for Use of Electronic Records in Clinical*** | ***September 2003*** | ***Organisations involved in clinical investigations of medical products:*** | ***Natural person*** | ***Food and Drug Administration (FDA)*** | ***While 21 CFR Part 11 remains in force, the FDA stated that it does not intend to actively enforce*** | ***Entities' systems should guarantee precision, dependability, and consistency of performance; limit*** | ***Mandatory protection levels and min.*** |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| ***Investigations (FDA), 21 CFR Part 11*** | | ***clinical investigators, sponsors, contract research organisations (CROs), and institutional review boards (IRBs)*** | | | ***certain provisions, such as those related to system validation, audit trails, record retention, and copying, provided that records remain trustworthy and reliable. However, the FDA may still take enforcement action if records are not properly maintained or submitted in accordance with applicable regulations.*** | ***authorized users' access to system, audit logs; establish and uphold written rules that hold people responsible and provide training. IT systems should be scrutinised, including any electronic systems used to create, edit, maintain, archive, retrieve, or transmit documents utilized in clinical trials.*** | ***technical standards*** |
| Securities and Exchange Act of 1934, updated by Section 409 of Sarbanes-Oxley Act of 2002 | August 23, 2004 | Publicly listed firms | Shareholder | SEC | Civil penalties can range from USD 25k to USD 500k or more. For severe cases, a firm's Exchange Act registration may be revoked | Requires mandatory notification about unscheduled major events important for shareholders within 4 business days | Data breach notification and fines |
| Defence Federal Acquisition Regulation (DFAR), 48 CFR 252.204-7012 | Oct. 1, 2015 | (Sub)contractors of Dpt of Defence (DoD) | State | Dpt.of Defence (DoD) | Debarment in case of non-compliance. | Requires (sub)contractors of DoD to ensure strict security to protect "covered Defence information" on unclassified information systems in case they hold, store, or transfer this information. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 is the cybersecurity standard to be followed | Mandatory protection levels and minimum technical standards |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| **Cybersecurity Information Sharing Act (CISA)** | **December 18, 2015** | **Federal agencies, private companies, information-sharing organisations** | **Natural and legal person (via reduced cyber risk)** | **Department of Homeland Security (DHS); U.S. Attorney General** | **No direct fines; provides liability protection** | **Facilitates sharing of cyber threat indicators (CTIs) and defensive measures between government and private sector. Offers liability protection for sharing information in good faith.** | **Cyber threat information governance and incident response coordination** |
| Consumer Privacy Protection Act of 2017 (CPPA) | Proposed 10/19/2017, not enacted | Businesses that, in any 12-month period, collect, use, access, transmit, retain, or discard sensitive personally identifiable information of 10k or more U.S. citizens. | Natural person | Department of Justice | Unless infraction is deliberate or purposeful, in which case an extra USD 5 m. can be levied, civil penalty sanctions cannot exceed USD 5 m. | Safeguards privacy and security of sensitive personal data, prevents and lessens identity theft, notifies people when their sensitive personal data is compromised, and improves law enforcement cooperation and other safeguards against security lapses, unauthorized access, and misuse of personal data. | Data breach notification and fines |
| ***CLOUD Act*** | ***March 23, 2018*** | ***All electronic communication service or remote computing service providers that operate in U.S.*** | ***Natural or legal person*** | ***Foreign and U.S. investigators.*** | ***N/A*** | ***Enhances procedures for both foreign and U.S. investigators in obtaining access to electronic information held by service providers.*** | ***Mandatory protection levels and minimum technical standards*** |
| ***Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)*** | ***Enacted March 2022; rulemaking ongoing*** | ***Critical infrastructure owners/operators*** | ***National cyber resilience, public*** | ***CISA (Department of Homeland Security)*** | ***TBD under rulemaking*** | ***Mandatory cyber incident and ransomware reporting*** | ***Reporting requirements*** |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| ***SEC Cybersecurity Disclosure Rule*** | ***Effective December 2023*** | ***Publicly listed firms*** | ***Investor and market participant*** | ***SEC*** | ***Civil penalties for non-compliance; enforcement discretion*** | ***Requires disclosure of material cybersecurity incidents within 4 business days and annual reporting on cyber governance*** | ***Data breach notification and fines*** |
| **Protecting Americans' Data from Foreign Adversaries Act (PADFAA)** | **June 2024** | **U.S. data brokers and processors dealing with foreign adversaries** | **Natural person (U.S. residents)** | **FTC** | **Civil penalties (aligned with FTC Act)** | **Authorises FTC to block transactions of sensitive personal data to entities tied to foreign adversaries** | **Data sovereignty and breach protection** |
| FTC Cybersecurity Guidance (Dec 2024) | December 2024 | Businesses, software developers, consumer-tech firms | Consumer, end-user | Federal Trade Commission | Enforcement under FTCA Section 5 | Secure-by-design, data protection best practices | Non-binding guidance |
| H.R.7535 – Quantum Computing Cybersecurity Preparedness Act | Introduced 2023; pending | Federal agencies, quantum tech developers | U.S. national security, user of quantum tech | NIST; DoD/DHS guidance bodies | N/A | Standards for quantum computing cybersecurity preparedness | Technical guidance framework |
| **NY DFS Cybersecurity Regulation Amendments** | **2024** | **New York-chartered financial institutions** | **Customer, financial system** | **NY Department of Financial Services** | **Civil penalties; license actions** | **Pen-testing, IR testing, encryption standards** | **Mandatory protection levels & standards** |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| HHS Updates to HIPAA Security Rule (2024) | Late 2024 (effective TBD) | Covered entities & business associates in healthcare | Patients' data privacy | HHS Office for Civil Rights (OCR) | Tiered: up to $1.5M/violation type | Cybersecurity enhancements, MFA, encryption, risk assessments | Mandatory protection levels & standards |

## Panel B: European Regulation

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| Data Protection Directive (95/46/EC) | October 1995 | Natural or artificial person, public authority or agency | Natural person | National Data Protection Authorities (DPAs) in each Member State | N/A | Regulates processing of personal data within EU and free movement of such data. | Data breach notification and fines |
| ***Network and Information Systems (NIS) Directive (EU/2016/1148)*** | ***2016 (Superseded by NIS 2 Directive (EU/2022/2555; on 16 Jan. 2023. Member States must transpose by 17 Oct. 2024.)*** | ***Banking and insurance, health, transportation and traffic, energy, water, and food sectors.*** | ***State*** | ***National competent authorities; CSIRTs; ENISA coordination*** | ***Not harmonised administrative fines; Member States establish own rules on penalties for non-compliance (leading to divergence in enforcement practices across the EU).*** | ***To establish consistent legal framework for cybersecurity. Member states should to develop adequate technological and organisational measures, safeguard national networks, and implement Directive. For operators of vital services and digital service providers, min. standards and security incident reporting duties are imposed.*** | ***Mandatory protection levels and min. technical standards*** |
| EU-U.S. Privacy Shield Framework for Protection of Personal Data Transferred from the EU to U.S. | July 12, 2016, invalidated on July 16, 2020 in Schrems II case (declared that it | U.S. businesses | EU citizens | U.S. Federal Trade Comm. and U.S. Dpt of Transportation | Civil penalties up to USD 40k per violation or USD 40k per day for continuing violations | Safeguards information of EU citizens kept and processed by businesses in U.S. | Data breach notification and fines |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| | did not provide adequate protection for personal data of EU citizens). | | | | | | |
| ***General Data Privacy Regulation (GDPR) (EU 2016/679 of EP and EC of 27 April 2016 on protection of natural persons wrt processing of personal data and on free movement of such data, and repealing Directive 95/46/EC)*** | ***25 May 2018*** | ***Co's established in EU processing personal data, or co established outside EU offering goods/services (paid or for free) or monitoring behaviour of individuals within EU.*** | ***Natural person*** | ***National Data Protection Authorities (DPAs); European Data Protection Board (EDPB) coordination*** | ***Fines of up to EUR 20 million, or 4% of worldwide turnover over preceding fin. year – whichever is higher*** | ***Rules relating to protection of natural persons wrt processing of personal data and rules relating to free movement of personal data.*** | ***Data breach notification and fines*** |
| ***Cybersecurity Act, Regulation (EU 2019/881 of EP and of EC of 17 April 2019) on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU 526/2013, Cybersec. Act)*** | ***June 2019*** | ***IT infrastructure*** | ***State*** | ***EU Agency for Cybersecurity (ENISA)*** | ***Member states shall lay down rules on penalties applicable to infringements of Act and to infringements of European cybersecurity certification schemes*** | ***IT products, services and processes consider cybersec. requirements and implement them at development stage. Creates European framework for cybersec. certification, categorization of IT products, services (low, mid, and high security categories).*** | ***Mandatory protection levels and min. technical standards*** |
| Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of | June 2019 | Public sector | Natural person | National authorities must ensure EU Comm. laws are correctly applied. | N/A | To increase accessibility of public sector data and establish regulations for reuse across all of Europe, by requiring member states to make documents reusable and by | Data breach notification and fines |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| public sector information | | | | | | defining and designating "high-quality data sets". | |
| ***The Digital Services Act (DSA)*** | ***In force since 16 November 2022; fully applicable from 17 February 2024*** | ***Online intermediaries, hosting services, online platforms, very large online platforms (VLOPs) and very large online search engines (VLOSEs)*** | ***Natural person, legal person*** | ***National Digital Services Coordinators (DSCs); European Commission (for VLOPs/VLOSEs)*** | ***Up to 6% of global annual turnover; daily fines for non-compliance*** | ***Establishes obligations for online platforms to remove illegal content, ensure transparency of ads and algorithms, protect fundamental rights and improve oversight*** | ***Mandatory protection levels and minimum technical standards*** |
| ***The Artificial Intelligence Act (AIA)*** | ***Adopted Dec 2023; phased applicability starting 2025*** | ***Developers, deployers, importers and distributors of AI systems in the EU*** | ***Natural person*** | ***National supervisory authorities designated by Member States, coordinated by the European AI Office*** | ***Up to €35 m. or 7% of global annual turnover for serious violations (e.g. use of prohibited AI); lower tiers for other non-compliance*** | ***Classifies AI by risk (unacceptable, high, limited, minimal), sets obligations for each category; prohibits social scoring and enforces transparency, human oversight, and robustness for high-risk AI*** | ***Data breach notification and fines*** |
| ***The Digital Markets Act (DMA)*** | ***In force since 1 November 2022; applicable from 2 May 2023*** | ***Core platform services designated as "gatekeepers" (e.g. large online platforms)*** | ***Business user, consumer, and smaller competitor*** | ***European Commission*** | ***Up to 10% of global annual turnover (20% for repeat violations)*** | ***Aims to ensure fair competition in digital markets; bans practices such as self-preferencing, restricts combining of personal data across services without consent*** | ***Data breach notification and fines*** |
| EUCC Certification Scheme (Regulation 2024/482) | 31 Jan 2024 | ICT product manufacturers and suppliers | Public authorities, businesses, end-user | National certification bodies; ENISA coordination | Voluntary – no fines | Cybersecurity certification of ICT products | Certification standards |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| ***Digital Operational Resilience Act (DORA)*** | ***In force since 16 January 2023; applies from 17 January 2025*** | ***Financial entities including banks, insurance companies, investment firms, crypto-asset service providers, and ICT third-party service providers*** | ***Financial system and its participants (including customers and institutions)*** | ***National competent authorities (e.g. ECB, ESAs, NCAs)*** | ***Administrative fines may be imposed in line with sector-specific regulations; critical ICT third-party providers can face fines up to 1% of average daily worldwide turnover*** | ***Establishes a harmonised framework for managing ICT risk in the financial sector. It mandates robust cybersecurity, incident reporting, digital resilience testing, and oversight of ICT third-party risk*** | ***Cybersecurity, ICT risk management, resilience, and compliance standards*** |
| Data Governance Act (DGA) | 2023 | Firms (data owners) | Natural and legal person | National authorities. | N/A | Aims to strengthen procedures to increase data availability, boost trust in data sharing, and remove technical barriers to data reuse. Establishment and growth of common European Data spaces in strategic domains, involving both public and private players. Strategic domains include health, environment, energy, agriculture, mobility, finance, manufacturing, public admin., and skills sectors. | Data breach notification and fines |
| ***The Data Act (DA)*** | ***Adopted 13 February 2024; enters into force 12 September 2025*** | ***Data holders (manufacturers, service providers), data users, public bodies*** | ***Natural and legal person (especially SME and consumer)*** | ***Competent national authorities; European Commission (coordination)*** | ***Member States define national penalties; must be effective, proportionate, dissuasive*** | ***Rules on Business-to-Business (B2B) and Business-to-Government (B2G) data access, and cloud service switching*** | ***Data breach notification and fines*** |
| ***Cyber Resilience Act (CRA)*** | ***In force 10 December 2024; obligations apply from 10 December 2027*** | ***Manufacturers, importers, and distributors of products with digital elements*** | ***End user (consumer and organisation)*** | ***Market surveillance authorities of Member States, coordinated by*** | ***Non-compliance with essential cybersecurity requirements: up to €15 m. or 2.5% of global turnover; other violations: €10 m. or*** | ***Introduces mandatory cybersecurity requirements across product life cycles for digital products (hardware /software); includes secure design, vulnerability*** | ***Mandatory protection levels and minimum technical standards*** |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| | | | | *the European Commission* | *2%; misleading info: €5 m. or 1%* | *management, and transparency* | |
| **Cyber Solidarity Act** | **Applies since 4 February 2025** | **Member states; national & cross-border Security Operation Centres (SOCs); "trusted providers" in critical sectors (health, energy, transport)** | **EU Member States, critical infrastructure sectors, and EU-wide cybersecurity resilience** | **European Commission (coordination); ENISA; designated national authorities** | **No direct monetary fines, but non-compliance may result in exclusion from EU Cybersecurity Reserve and related crisis support services** | **Establishes a European Cybersecurity Alert System; Cybersecurity Emergency Mechanism (including an EU Cybersecurity Reserve of certified private providers); and an Incident Review Mechanism to improve detection, response, support, recovery, and shared learning from large-scale cybersecurity incidents** | **Regulation (EU) - horizontal cybersecurity & crisis response** |
| **EU-US Data Privacy Framework** | **10 July 2023** | **U.S.-based companies certified under the framework that receive personal data from the EU** | **Individuals (EU citizens) whose personal data is transferred abroad** | **U.S. Dpt. of Commerce (certification oversight); U.S. FTC (enforcement); EC (adequacy decision)** | **No fines specified, but U.S. co's are subject to enforcement under Section 5 of FTC Act (prohibits unfair or deceptive actions). Non-compliance can lead to FTC enforcement actions, including civil penalties. On European side: EU-based data exporters remain subject to GDPR. If they transfer data to U.S. co's not in compliance with framework, they may face GDPR-level fines imposed by their national** | **Establishes conditions and oversight mechanisms for lawful transfer of personal data from EU to U.S.; provides redress mechanisms and oversight structures** | **Data breach notification and fines** |

| Name of law | Effective date | Targeted subjects | Beneficiary of regulation | Enforcement agency | Fines/penalties | Subject matter of the law | Type |
|---|---|---|---|---|---|---|---|
| | | | | | **data protection authorities.** | | |
| ***NIS2 Directive (Directive (EU) 2022/2555)*** | ***Enacted 27 December 2022; transposed in national regulations by Member States by 17 October 2024*** | ***Essential and important entities across energy, transport, banking, health, digital infrastructure, etc.*** | ***State, citizen, critical service user*** | ***National competent authorities; CSIRTs; coordinated at EU level by ENISA*** | ***Up to €10 million or 2% of global annual turnover*** | ***Expands scope and enforcement of cybersecurity requirements and incident reporting across more sectors; strengthens national and EU-wide coordination*** | ***Mandatory protection levels and minimum technical standards*** |
| European Health Data Space (EHDS) | In force 26 March 2025 | Health data holders, healthcare providers | EU citizen and researcher | National health data access bodies; EU oversight | Penalties under national laws | Enables access and reuse of electronic health data across EU, with strict privacy and governance rules | Data breach notification and fines |
| Digital Networks Act (DNA) | Expected Q4 2025 publication; full applicability TBD | Telecom & connectivity providers; national regulators | Consumer, business, entire digital ecosystem | National telecom regulators; coordinated by EC | TBD | Harmonisation of spectrum, infrastructure investments, telecom regulation | Connectivity/infrastructure regulation |

## Appendix 3. U.S. Data Breach State Legislation[84]

This table provides information about data breach notification laws per state: year of introduction, reporting threshold (magnitude of affected/compromised individuals), and penalties (max. possible penalty following data breach, if available).

| State | Start | Minimum, Reporting Threshold | Min Threshold | Penalty (USDk) |
|---|---|---|---|---|
| CA | 2002 | If notice is provided to more than 500 CA residents, the entity must also notify the Attorney General. | 500 | 250 |
| AR | 2005 | Notification must be made in the most expedient time and manner possible without unreasonable delay. Notification is not required if investigation determines that there is no reasonable likelihood of harm to affected individuals. | N/A | N/A |
| CT | 2005 | Notification is not required if investigation, along with consultation with relevant government agencies, determines that there is no reasonable likelihood that breach will result in harm to affected individuals. | N/A | N/A |
| DE | 2005 | Notification is not required if, after appropriate investigation, the entity reasonably determines breach is unlikely to result in harm to affected individuals. | N/A | N/A |
| GA | 2005 | If more than 10,000 Georgia residents have to be notified of a breach, breached entities must also inform all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C Section 1681a, without unreasonable delay. | 10000 | N/A |
| IL | 2005 | Breached third parties must notify the relevant data owners or licensees immediately following discovery. | N/A | N/A |
| ID | 2005 | If more than 1,000 individuals must be notified of breach, breached entities must also inform all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C Section 1681a(p). | 1000 | 150 |
| LA | 2005 | Notice must be made without unreasonable delay, but no later than 60 days following discovery of breach. | N/A | 5 |
| ME | 2005 | If more than 1,000 individuals must be notified of a breach, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C Section 1681a(p). | 1000 | 2.5 |
| MN | 2005 | If more than 500 individuals must be notified, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C Section 1681a, within 48 hours. | 500 | N/A |
| NV | 2005 | If more than 1,000 individuals must be notified, breached entities must also notify all consumer reporting agencies. | 1000 | N/A |
| NJ | 2005 | If more than 1,000 individuals must be notified, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C Section 1681a. | 1000 | N/A |
| NY | 2005 | If more than 5,000 residents must be notified, breached entities must also notify consumer reporting agencies. | 5000 | 150 |
| NC | 2005 | If more than 1,000 residents must be notified, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C Section 1681a(p). | 1000 | N/A |
| ND | 2005 | Breached third parties must notify relevant data owners or licensees immediately following discovery of breach. | N/A | N/A |

| State | Start | Minimum, Reporting Threshold | Min Threshold | Penalty (USDk) |
|---|---|---|---|---|
| OH | 2005 | If more than 1,000 individuals have to be notified of breach, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, unless they are covered by HIPAA. | 1000 | N/A |
| TN | 2005 | If more than 1,000 individuals must be notified, breached entities must notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. | 1000 | N/A |
| WA | 2005 | If more than 500 residents must be notified, entity must also electronically submit a sample copy of breach notification to Attorney General, along with number of Washington consumers affected by breach. Breached third parties must notify relevant data owners or licensees immediately following discovery of the breach. | 500 | N/A |
| AZ | 2006 | Entities must notify Attorney General in writing if entity is required to notify more than 1,000 residents. | 1000 | 500 |
| CO | 2006 | If notice is provided to more than 1,000 residents, entity must also notify all consumer reporting agencies that compile and maintain | 500 | N/A |
| HI | 2006 | If more than 1,000 individuals must be notified, Hawaii's Office of Consumer Protection must also be notified, as must all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C Section 1681a(p). | 1000 | 2.5 |
| ID | 2006 | Notice shall be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of breach, identify affected individuals, and restore reasonable integrity of data system(s). State agencies must inform the office of the Idaho Attorney General within 24 hours of the discovery of a data breach. | N/A | 25 |
| KA | 2006 | If more than 1,000 individuals must be notified of a breach, breached entities must also inform all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C Section 1681a(p). | 1000 | N/A |
| MI | 2006 | If more than 1,000 individuals must be notified, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C Section 1681a(p), unless they are subject to Title V of the GLBA. | 1000 | 750 |
| MT | 2006 | Notice must be made without unreasonable delay. An electronic copy of the notice, along with supporting information, must also be submitted to the Attorney General's consumer protection office. | N/A | N/A |
| NR | 2006 | Notice must be made without unreasonable delay, unless investigation determines it is unlikely the personal information will be used for unauthorized purposes. | N/A | N/A |
| NH | 2006 | If more than 1,000 individuals have to be notified of breach, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C Section 1681a(p) unless they are subject to Title V of the GLBA. | 1000 | N/A |
| PA | 2006 | If more than 1,000 individuals must be notified, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. | 1000 | N/A |
| RI | 2006 | If more than 500 residents must be notified, Attorney General must be notified, along with major credit reporting agencies. | 500 | N/A |
| UT | 2006 | Breached third parties must notify and cooperate with relevant data owners or licensees immediately following discovery of the breach. | N/A | 100 |
| VE | 2006 | If more than 1,000 residents must be notified, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. | 1000 | N/A |
| WI | 2006 | If more than 1,000 individuals must be notified, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. | 1000 | N/A |

| State | Start | Minimum, Reporting Threshold | Min Threshold | Penalty (USDk) |
|---|---|---|---|---|
| MD | 2007 | If more than 1,000 individuals must be notified, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on nationwide basis, as defined in 15 U.S.C Section 1681a(p). | 1000 | N/A |
| MA | 2007 | Breached entities must also inform Attorney General and director of consumer affairs and business regulation, who will then pass on any relevant information to consumer reporting agencies and state agencies. | N/A | N/A |
| OR | 2007 | If more than 250 individuals must be notified, breached entities must also notify Attorney General in same manner as consumers. | 250 | N/A |
| TX | 2007 | If more than 10,000 individuals must be notified, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on nationwide basis. | 1000 | 250 |
| WY | 2007 | Breached third parties must notify relevant data owners or licensees as soon as practicable. If breached third parties do not agree to notify affected individuals, the responsibility of notification falls on the data owner or licensee. | N/A | N/A |
| AK | 2008 | If more than 1,000 individuals have to be notified of breach, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on nationwide basis | 1000 | 50 |
| IA | 2008 | If more than 500 individuals must be notified of a breach, breached entities must also notify the director of the consumer protection division of the Attorney General's Office within five days of notice being given to affected individuals. | 500 | N/A |
| OK | 2008 | Breached third parties must notify the relevant data owners or licensees as soon as practicable. | N/A | 150 |
| SC | 2008 | If more than 1,000 individuals must be notified, breached entities must notify Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. | 1000 | 1 |
| VA | 2008 | If more than 1,000 individuals must be notified, breached entities must also alert all consumer reporting agencies and Attorney General as to the notification. | 1000 | 150 |
| WV | 2008 | If more than 1,000 individuals must be notified, breached entities must also notify all consumer reporting agencies. | 1000 | N/A |
| MO | 2009 | If more than 1,000 individuals must be notified, breached entities must also notify Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C Section 1681a(p). | N/A | N/A |
| MS | 2010 | Breached third parties must notify the relevant data owners or licensees as soon as practicable following discovery of breach. Substitute notice is permitted in specific circumstances and notification may be delayed for law enforcement purposes. | N/A | N/A |
| FL | 2014 | If more than 1,000 individuals are affected, breached entities must also inform all consumer reporting agencies that compile and maintain files on consumers on nationwide basis, as defined in 15 U.S.C Section 1681a(p), without unreasonable delay. | 1000 | 50 |
| KY | 2014 | If more than 1,000 individuals must be notified of breach, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on nationwide basis, as defined in 15 U.S.C Section 1681a(p). | 1000 | N/A |
| NM | 2017 | If notice must be provided to more than 1,000 residents, notice must also be given to Attorney General and all consumer reporting agencies that compile and maintain files on consumers on nationwide basis. The notice must include the number of New Mexico residents affected and include a copy of the notice that went to affected residents. | 1000 | N/A |
| AL | 2018 | Less than 1000 residents: notice to be sent to all affected. More than 100: consumer reporting agency to be alerted. | 100 | 500 |

| State | Start | Minimum, Reporting Threshold | Min Threshold | Penalty (USDk) |
|---|---|---|---|---|
| SD | 2018 | If more than 250 residents must be notified, breached entities must also notify Attorney General. | 250 | 10 |

## about ECGI

The European Corporate Governance Institute has been established to improve *corporate governance through fostering independent scientific research and related activities.*

The ECGI will produce and disseminate high quality research while remaining close to the concerns and interests of corporate, financial and public policy makers. It will draw on the expertise of scholars from numerous countries and bring together a critical mass of expertise and interest to bear on this important subject.

The views expressed in this working paper are those of the authors, not those of the ECGI or its members.

ECGI Working Paper Series in Law



https://ecgi.global/content/working-papers

**Electronic Access to the Working Paper Series**

The full set of ECGI working papers can be accessed through the Institute's Web-site (https://ecgi.global/content/working-papers) or SSRN:

| | |
|---|---|
| **Finance Paper Series** | http://www.ssrn.com/link/ECGI-Fin.html |
| **Law Paper Series** | http://www.ssrn.com/link/ECGI-Law.html |