nebul

RISKS AND COMPLIANCE CONSIDERATIONS

An Overview of the impact of EU laws on Cloud Services and Public Clouds: EU and U.S. legal framework for public cloud services: Risks and Compliance consideration.

Version: 01-07-2025

In close cooperation with

BarentsKrans

Table of Contents

Version Table

Version	Date	Status	Information
1.0	01-07-2025	Published	Nebul lay-outs
0.9	30-06-2025	Concept version	Setting up legal content by BarentsKrans

I INTRODUCTION

1 In the past decade, the regulatory landscape in the digital sector of the European Union (**EU**) has undergone a fundamental and rigorous transformation. From the adoption of the General Data Protection Regulation (**GDPR**) in 2016 to the entry into force of the Artificial Intelligence Act (**AI Act**) in 2024, a wide range of legislative efforts have been enacted in the EU that regulate multiple aspects of the EU digital market.

2 Simultaneously, digital service providers have increasingly adapted their business models from offering 'on-premise' software services, to cloud-based software offered from a distance through the internet (**Cloud Services**). Cloud Services have become an attractive option for both providers and their customers relative to on-premise solutions; they generally offer a less expensive, accessible, scalable and innovative method for software and hardware products used by organisations.

3 Currently, Cloud Services are most often provided through public cloud environments (**Public Cloud**). In Public Clouds, the resources required to provide Cloud Services (such as servers and storage) are provided through infrastructures that are owned and managed by the Cloud Service provider (**CSP**) and is shared by all recipients of those Cloud Services. This provides CSPs the option to scale up or down efficiently, reduce costs and have centralized locations for data storage.[1]

4 However, the steep rise and integration of Cloud Services is also cause for concern, particularly from the perspective of EU digital sovereignty, continuity safeguards and data protection and privacy rights for EU citizens.[2] The majority of (large) CSPs have their main establishment, infrastructure and operational management in the United States (**U.S.**). The U.S. has gradually increased the competences of federal and local law enforcement and investigatory authorities (**U.S. Authorities**) to access data transferred and stored within and outside its territorial jurisdiction.[3]

5 Accordingly, although Cloud Services have become one of the most widely-used digital infrastructure by both public and private entities established in the EU (**EU Entities**), they have simultaneously become one of – if not the – most regulated components of the digital market. Not only general, technology-neutral legislation regarding access, storage and transfers of increasingly more categories of data, but also specific sectoral legislation on the safety, security and continuity of IT infrastructures has been adopted to mitigate risks for (unlawful) access, be it by U.S. Authorities or unauthorized individuals, and to protect EU digital sovereignty against overdependence and overreliance on U.S. Cloud Services.

6 This document aims to provide a (non-exhaustive) overview of the impact of EU laws on Cloud Services and Public Clouds, the legal framework enabling U.S. Authorities to access data processed with Public Clouds and Cloud Services, and the resultant risks and compliance considerations for EU Entities.

---

1 Dutch General Court of Auditors 2025, 'Het Rijk in de cloud', p. 19 – 20.
2 *Ibid.*, p 21 – 22.
3 *Ibid.* p. 23 – 26.

7 Chapter II summarises the key risks and compliance considerations for EU Entities when using Cloud Services offered by U.S. CSPs, particularly regarding data access rights by U.S. Authorities and the concentration risks associated with using large (U.S.) CSPs. Chapters III and IV provide a non-exhaustive overview of the EU legal framework applicable to Cloud Services used by EU Entities and the U.S. laws providing access to data by U.S. Authorities respectively.

8 In summary, the diversity and fragmented nature of the legal framework applicable to Cloud Services makes it imperative that EU Entities do their due diligence on the foreseeable risks, applicable obligations and compliance issues when looking to use Cloud Services and/or migrate their data to a Public Cloud. This is all the more pressing in case of Cloud Services and Public Clouds offered by CSPs within the jurisdiction of the U.S. authorities. Not only the federal U.S. government, but individual U.S. States too have adopted laws allowing local U.S. Authorities access to data transferred and stored in their state territory (**State Surveillance Laws**), creating a complex, layered and fragmented patchwork of legal acts that both U.S. CSPs and EU Entities must navigate through.

9 This advice is addressed to Nebul B.V. and may relied upon only by Nebul B.V., subject to the terms of the engagement between Nebul and BarentsKrans Coöperatief U.A. If (portions of) this advice are reused or shared with third parties, such third parties have no reliance on this document and it should not be construed as legal advice by BarentsKrans Coöperatief U.A. to such parties.

II RISKS AND COMPLIANCE CONSIDERATIONS WHEN CONTRACTING WITH U.S. PUBLIC CLOUD SERVICES PROVIDER

II.1 Loss of control over data: (Unlawful) access by U.S. Authorities

10 The engagement of U.S. CSPs creates several challenges for EU Entities to comply with their obligations under EU data protection and privacy laws. For example, the storage of personal data on Public Clouds located in the U.S. and operated by U.S. CSPs qualifies as a transfer under the GDPR, meaning EU Entities must comply with the GDPR rules on data transfers[4] and ensure that the level of data protection warranted in the EU is also provided in the U.S.[5]

11 Under the Clarifying Laws On Use of Data Act (**CLOUD Act**) U.S. CSPs can be obligated to comply with warrants from U.S. Authorities to disclose data in their possession, custody, or control, even when the data is not stored on Public Clouds in the U.S. CSPs can object to such warrants when the person whose data is ordered is not a U.S. citizen and does not reside in the U.S. and "*the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.*" A foreign government is "*qualifying*" if it concluded a bilateral agreement on mutual data sharing with the U.S. At the time of writing, no such agreements have been concluded with the EU or any of its member states, meaning CSPs are currently not able to challenge a warrant issued by U.S. Authorities for data relating to EU individuals on this basis.

4 Chapter V GDPR.
5 See section III.1.1.

12 Similarly, Section 702 of the Foreign Intelligence Surveillance Act (**Section 702 FISA**) and Executive Order 12333 (**E.O. 12333)** have been critiqued for lacking effective judicial redress and supervision on individual cases by competent authorities. While the Foreign Intelligence Surveillance Court (**FISC**) is responsible for reviewing the conduct of the NSA under Section 702 FISA, it cannot reject or investigate individual orders of the NSA; the FISC is merely able to review the procedures used to determine which individuals are targeted in a broad sense. Conduct of the NSA under the guise of E.O. 12333 has in the past been found to lack judicial remedies and oversight as it does not confer rights which are enforceable against U.S. Authorities.

13 The adoption of Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence (**E.O. 14086**) on 7 October 2022 strengthened the conditions, limitations and safeguards that apply to surveillance activities of U.S. Authorities on the basis of, amongst others, Section 702 FISA and E.O. 12333. E.O. 14086 also led to the establishment of the Privacy and Civil Liberties Oversight Board (**PCLOB**), offering a new redress mechanism through which non-U.S. citizens can submit and resolve complaints concerning unlawful access to their data by U.S. Authorities. On this basis, the European Commission adopted the Data Privacy Framework (**DPF**)[6] adequacy decision, which is currently in effect.

14 Although the DPF enables the transfer of personal data to U.S. CSPs that are DPF-certified without any additional safeguards[7], doubts have been expressed on the long-term viability of the DPF given the current U.S. political climate and the way the DPF safeguards have been put in place (through executive orders "only") and. Recent actions by the current U.S. administration, as well as possible future developments may undermine the protection of the DPF-safeguards and, by extension, those in E.O. 14086.[8]

15 The adequacy decisions for EU – U.S. data transfers have been annulled twice by the Court of Justice of the European Union (**CJEU**).The CJEU concluded that the level of data protection provided by the U.S. was inequivalent to that in the EU, mainly due to the lack of redress measures in Section 702 FISA and E.O. 12333.[9] Non-Governmental Organisation NOYB, which has successfully litigated against the earlier EU – U.S. adequacy decisions, has already issued a statement that it intends to challenge the DPF.[10]

6 Commission Implementing Decision EU 2023/1795 on the adequate level of protection of personal data under the EU-US Data Privacy Framework.
7 Article 45 GDPR.
8 See for example the termination of contracts of the Democratic members of the PCLOB by the U.S. government on January 27, 2025, Bloomberg January 28 2025, Trump Fires Trio of Democrats from Privacy Oversight Board.
9 CJEU 6 October 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems I*); CJEU 16 July 2020, C-311/18 (*Schrems II*).
10 NOYB 10 July 2023, European Commission gives EU-US data transfers third round at CJEU. See also its response to the decision by the current U.S. administration to remove the Democratic members of the PCLOB: NOYB 23 January 2025, US Cloud soon illegal? Trump punches first hole in EU-US Data Deal.

16 Additionally, U.S. CSPs must impose adequate technical, organisational, legal and contractual safeguards to limit access to non-personal data as much as possible in accordance with the Data Act and Data Governance Act.[11] If a U.S. court or authority compels a U.S. CSP to transfer or give access to non-personal data, absent an agreement between the EU and U.S., the CSP may share or give access to that data if (i) the decision is proportionate and sufficiently specific; (ii) the CSP can object to a competent court; and (iii) that competent court is empowered to take due account of EU or EU member state law requirements conflicting with the order to share the data.

17 In light of the above, EU Entities should exercise caution and do proper due diligence when considering to move their data to Public Clouds managed and operated by U.S. CSPs.

II.2 Dependence on U.S. Public Clouds: concentration and continuity risks ("vendor lock-in")

18 Another issue that has been addressed by public sector and supervisory authorities is the risk of overreliance on (a select few) CSPs for business continuity purposes. If outsourcing through Cloud Services forms the bulk of an EU Entities' IT infrastructure, it may lose control and oversight of where data is located and which measures are taken to guarantee that appropriate safeguards and protection exist. In case the physical infrastructure for Public Clouds is not operated in the EU, but in third countries, this risk is even more apparent and may lead to concentration risks, continuity issues, and *vendor lock-in*.

19 Concentration and continuity risks arise when the bulk of an EU Entity's (critical or important) IT services is provided by only a handful of (large) CSPs. Specifically in the case of CSPs under the jurisdiction of the U.S., the current geopolitical climate requires that EU Entities seriously contemplate the potential effects of international sanctions imposed by the U.S. government. Such sanctions can force CSPs under the jurisdiction of the U.S. to cease the provision of, or deny access to, their Cloud Services and Public Clouds.

20 A recent example of such risks potentially materialising is seen in the context of the sanctions imposed by the U.S. against certain members of the International Criminal Court (**ICC**). There are reports that Microsoft's Cloud Services are critical for the ICC. According to those reports, the ICC stores essentially all the evidence in the cases it handles on Microsoft's Azure cloud platform.[12] The sanctions allow that assets in the U.S. of any natural or legal persons which have provided technological support for, or goods or services to or in support of the activities of the ICC may be frozen.[13] As such, Microsoft's own interests in preventing being caught by these sanctions may lead to a shutdown of access to the Azure platform by the ICC, effectively blocking it from performing its tasks and operations.[14] Similar concerns arise in the context of (Dutch) banks providing banking services to the ICC.[15]

21 The EU legislator has attempted to align the interests of CSPs and important and/or essential EU Entities by qualifying the former as important or essential entities (depending on their size) themselves in NIS 2.[16, 17] Accordingly, these providers will need to comply with NIS 2 on their own accord by implementing robust policies for the security of network and

---

11 See sections III.1.2 and III.1.3.
12 The Guardian 20 January 2025, ICC braces for swift Trump sanctions over Israeli arrest warrants.
13 White House 9 February 2025, Imposing sanctions on the International Criminal Court.
14 We refer to the dispute around the Amsterdam Trade Bank where Microsoft refused to grant the liquidators in the bankruptcy access to the cloud environment. See: Amsterdam District Court 3 May 2022, ECLI:NL:RBAMS:2022:4452.
15 Dutch Broadcasting Foundation 7 February 2025, Kabinet al weken op zoek naar oplossing sancties Strafhof (Dutch only).
16 See section III.2.1.
17 See Annex I of NIS 2.

information systems and report significant incidents to the competent supervisory authorities themselves.

22 In the financial sector, the DORA[18] imposes stringent due diligence obligations on financial entities looking to migrate (part) their digital assets to (Public) Cloud Services. Complying with these obligations may become challenging when Cloud Services are provided by U..S. CSPs, as the receiving financial entities may not have (or be provided) all necessary information to conduct due diligence on the risks involved with specific Cloud Services. The DORA also imposes specific contractual stipulations that must be included in contracts with CSPs, particularly where they provide Cloud Services that support critical or important functions from the perspective of the financial entity. These mandatory contractual provisions include the effective rights to perform audits and access to data. Other considerations for financial entities to be aware of are concentration risks and the loss of control over security of the supply chain in the case of U.S. CSPs. The DORA requires EU financial entities to assess these risks and explore alternative solutions that would diminish (over)exposure to the same CSPs, for example by engaging different, EU-established CSPs for IT services supporting their critical or important functions.

23 Executives and management bodies of EU Entities under NIS 2 and/or the DORA are also compelled to take a proactive stance and responsibility for maintaining secure and transparent ICT and cybersecurity policies. A mere dereference to choices made by IT departments will no longer be sufficient for executives to meet their responsibilities under NIS2 and the DORA. Non-compliance with these responsibilities may result in personal liability of executives and board members for the damages caused[19, 20]

24 Lastly, the EHDS[21] will require EU Entities qualifying as healthcare providers to participate and adapt their current IT and electronic health record systems (**EHR Systems**) to be compliant with the product requirements stipulated in the EHDS and must be interoperable with harmonised software components of EHR Systems, MyHealth@EU and its national counterparts. By offering an EU-centralised platform operated by the EU and national regulated governments (i.e., MyHealth@EU and its national counterparts) the EU medical digital restructure is aimed at tackling and the fragmentation and reducing dependency on a small number of commercial (U.S.) CSPs.

25 Since the choice for a Public Cloud is generally intended to be made for a long term, and given the current volatile geopolitical landscape, EU Entities should exercise caution and do a proper due diligence assessment, especially when considering engaging with non-EU CSPs.

---

18 See section 0.

19 In the Netherlands, the principle of liability of board members and executives is codified in Article 2:9 of the Dutch Civil Code. This principle goes beyond the requirements in NIS 2 an/or the DORA and applies to actions or negligence of board members that damage an organisation in a broader context. For board members to be personally liable, it has to be established that a serious reproach can be made for their acts or omissions.

20 In addition to NIS2 and the DORA, the Dutch Corporate Governance Code (**DCGC**) requires in article 1.2.1 that board members of publicly listed Dutch companies take responsibility for the identification and analysis of operational, compliance and reporting risks of their corporation. These risks include the stability and security of information and communications technology (such as Cloud Services), data protection, continuity, and concentration liabilities which are discussed in this memo.

21 See section 0

III EU LEGAL FRAMEWORK

26 As stated above, the EU has adopted and implemented multiple legal acts aimed at regulating the EU digital market and data economy which (also) apply to Cloud Services used by EU Entities. These laws are based on the general and fundamental rights to data protection and privacy on the one hand,[22] with specific sectoral laws aimed at protecting the stability and continuity of digital services used within certain essential and/or critical market segments on the other hand.

27 The following sections contain a non-exhaustive list of EU laws which form the framework for EU Entities when using (U.S.) Cloud Services and store their data in Public Clouds. Annex I provides a short summary of this chapter per legal act.

III.1 Data protection and privacy laws

III.1.1 GDPR[23]

28 The GDPR serves to regulate and protect the data and privacy of persons in the EU (**Data Subjects**) by laying down common and uniform rules regarding the processing and movement of personal data. Due to its direct effect in the legal order of all EU member states, it provides the basis for the free movement of personal data with the EU, while obligating EU Entities to warrant the level of protection.

29 The GDPR provides rights to Data Subjects whose personal data is processed and obligates that EU Entities responsible for the processing activity implement measures to guarantee that the data is processed in a secure and lawful manner. Some fundamental obligations imposed upon such EU Entities are the necessity of having a legal basis for personal data processing; the requirement to provide an adequate security level by implementing appropriate technical and organisational measures to protect personal data; and the requirement to prevent and notify any unauthorised access to or loss, unavailability and/or alteration of personal data.

30 The GDPR also distinguishes between certain categories of personal data which deserve more stringent protection and permits the processing thereof only under limited circumstances (**Special Categories of Personal Data**).[24] Examples of Special Categories of Personal Data are biometric and genetic data, data revealing racial or ethnic origin, and data concerning health. The processing of Special Categories of Personal Data is only allowed if a specific exemption applies, such as explicit consent from the Data Subject,[25] or necessary for the provision of health care.[26] Personal data relating to criminal offences is allowed only under the control of official authorities or if authorised by law.[27]

31 If a processing activity is likely to result in a high risk to the rights and freedoms of Data Subjects, the controller must perform a data protection impact assessment (**DPIA**).[28] Controllers will have to identify these risks and explain how they intend to mitigate them in the DPIA.[29] In the context of U.S. CSPs – particularly on Public Clouds – depending on the nature and volume of data stored (e.g., large sets of health or genetic data), there are several risks that may trigger the need to perform a DPIA, such as unauthorised access,

---

22 Articles 7 and 8 of the EU Charter of Fundamental Rights.
23 Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data (**GDPR**).
24 Article 9(1) GDPR.
25 Article 9(2(a) GDPR.
26 Article 9(2)(h) GDPR.
27 Article 10 GDPR.
28 Article 35 GDPR.
29 European Data Protection Board, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

loss of control over the data by the controller, or insufficient technical and/or organisational security measures taken by the CSP.

32 If an EU Entity transfers personal data to a non-EU country it is responsible to ensure that appropriate safeguards are in place so that the personal data continues to benefit from an adequate level of protection.[30] EU Entities remain responsible for compliance with the GDPR by CSPs that process personal data on their behalf. Storage of personal data on a Public Cloud hosted in the U.S. can be problematic as EU Entities may lose control and oversight over the technical security design of the Public Cloud, access rights to and the way personal data is used by the CSP.[31]

III.1.2 Data Act[32]

33 The Data Act is an EU legal act whose purpose is twofold. First, the Data Act contains rules on the sharing and use of data generated by Internet of Things-devices. Second, the Data Act prescribes legal procedures that facilitate the switching between data processing services (including Cloud Services) and aims to provide protection against unlawful governmental access to and transfers of non-personal data in third countries.

34 The Data Act compels providers of data processing services (such as CSPs) to take all adequate technical, organisational and legal measures to prevent transfers of, and access to non-personal data to government authorities of non-EU countries.[33] Judgements, courts orders or warrants of government authorities of third countries that obligate CSPs to provide access or transfer non-personal data (**Third-Country Orders**) are considered lawful only in cases of an international agreement concluded between the EU and that third country,[34] or if there are adequate safeguards to guarantee legal certainty and protection.[35]

35 CSPs must only provide the strict minimum amount of data required to comply with the Third-County Order.[36] They must also inform EU Entities about the existence of a Third Country Order, unless it concerns a purpose for law enforcement, but then only for as long as necessary to guarantee its effectiveness.[37]

36 These obligations will become applicable on 12 September 2025. Accordingly, CSPs should have implemented procedures to allow them to act in accordance with the Data Act by that date.

III.1.3 Data Governance Act[38]

37 The Data Governance Act provides a legal framework establishing the conditions for the (commercial) use of government data by third parties and the supervision of providers of data intermediary services, amongst which CSPs.

38 Under the Data Governance Act providers of data intermediary services must take all adequate technical, organisational and legal measures to prevent unlawful transfers of, and access to non-personal data to government authorities of non-EU countries.[39] Third-

30 Article 44 GDPR.
31 Dutch General Court of Auditors 2025, p. 39.
32 Regulation (EU) 2023/2854 on harmonized rules on depending on the nature and volume of data stored (e.g., large sets of health or genetic data) (**Data Act**).
33 Article 32(1) Data Act.
34 Article 32(2) Data Act.
35 Article 32(3) Data Act. See also paragraph 0 above.
36 Article 32(4) Data Act.
37 Article 32(5) Data Act.
38 Regulation 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (**Data Governance Act**).
39 Article 31(1) Data Governance Act.

Country Orders that obligate CSPs to provide access or transfer non-personal data are considered lawful only in cases of an international agreement concluded between the EU and that third country,[40] or if there are adequate safeguards to guarantee legal certainty and protection.[41]

39 CSPs may only provide the strict minimum amount of data required to comply with the Third-County Order.[42] They must also inform EU Entities about the existence of a Third Country Order, unless it concerns a purpose for law enforcement, but then only as long as necessary to guarantee its effectiveness.[43]

III.1.4 AI Act[44]

40 The AI Act aims to regulate development, distribution and usage of artificial intelligence (**AI**) in the EU and protect the health, safety, fundamental rights against its harmful effects. The AI Act divides AI systems into three categories, namely prohibited,[45] high-risk[46] and limited-risk AI systems.[47, 48] In the context of Cloud Services, the AI Act is most relevant for storage of data in Public Clouds generated by or used in connection with high-risk AI systems.

41 Providers of high-risk AI systems may process Special Categories of Personal Data to detect and mitigate biases in its output provided specific conditions are met.[49] One of those conditions is that those Special Categories of Personal Data are not transmitted, transferred or otherwise accessed by other parties such as CSPs that host that data in their Public Clouds.[50] Providers may face challenges to comply with this rule if using U.S. CSPs, as U.S. laws do allow access to U.S. Authorities to Special Categories of Personal data stored on Public Clouds.[51]

42 High-risk AI systems must also bear a CE-marking before being placed on the EU market.[52] One of the requirements for acquiring this CE-marking is a confirmation that the AI system complies (amongst others) with the GDPR.[53] This means that personal data transfers through high-risk AI systems to Public Clouds managed by CSPs in the U.S. must comply with all transfer obligations in the GDPR to get a CE-marking. Depending on the developments in respect of the DPF[54], this may be challenging to achieve in practice.[55]

43 The requirements for providers and deployers of high-risk AI systems will become applicable and enforceable on 2 August 2026.

40 Article 31(2) Data Governance Act.
41 Article 31(3) Data Governance Act.
42 Article 32(4) Data Governance Act.
43 Article 32(5) Data Governance Act.
44 Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (**AI Act**).
45 Article 5 AI Act.
46 Article 6, Annex I and Annex III AI Act.
47 Article 50 AI Act.
48 As well as General-Purpose AI Models; see Chapter V of the AI Act.
49 Article 10(5) AI Act.
50 Article 10(5)(d) AI Act.
51 See above section II.1 and Chapter IV below.
52 Article 47 AI Act.
53 Annex V AI Act.
54 See above section paragraphs 19 and 20.
55 See above section II.1.

III.2 Sector-specific cybersecurity laws

III.2.1 NIS 2[56]

44 NIS 2 aims to provide a high level of cybersecurity for network and information systems used by organisations active within market segments of critical importance to key societal and economic activities in the EU including but not limited to the healthcare, energy, banking and digital infrastructure such as Cloud Services.[57]

45 NIS 2 lays down minimum rules for the implementation of cybersecurity policies, business continuity plans and incident handling practices by EU entities qualifying as essential or important.[58] These entities must assess the risks associated with their network and information systems based on their direct suppliers and service providers.[59]

46 Entities within scope of NIS 2 must also report incidents (capable of) causing severe operational disruptions of the services they provide, or (im)material financial damages for them or third parties.[60] The deadline for reporting these incidents is short: only 24 hours after becoming aware of the incident must an initial report be filed.[61] This means EU Entities classifying as essential or important entities should make clear and binding agreements with CSPs to cooperate in the investigation and resolution of such incidents to comply with their own obligations.

47 NIS 2 creates obligations for management bodies of covered entities to ensure those entities comply with the substantive obligations of NIS 2. If this duty is breached, it may result in personal liability for board members.[62, 63]

III.2.2 DORA[64]

48 The DORA is a financial sector-specific EU regulation aiming to achieve a high level of digital operational resilience for financial entities in the EU. The DORA requires financial entities to identify, monitor and manage the risks and vulnerabilities associated with the use of third-party ICT service providers for their network and information systems.[65] Financial entities are furthermore obligated to report ICT-incidents that have a high adverse impact on their network and information systems.[66] Financial entities also need to include clear rights to audits, access to data and termination in the contractual arrangements with their ICT service providers .[67]

49 As mentioned above, ICT services are increasingly provided through (Public) Cloud Services, and as such, the DORA explicitly obligates financial entities to consider compliance with data protection laws as well as the laws of any non-EU country in which their CSPs are established.[68]

---

56 Directive 2022/2555 on measures for high common level of cybersecurity across the EU (**NIS 2**).
57 See Annex I and II NIS 2 for a full overview of all market segments.
58 Article 21 NIS 2.
59 Article 21(2)(d) NIS 2.
60 Article 23 NIS 2.
61 Article 23(4) NIS 2.
62 Articles 20(1) and 32(6) NIS 2.
63 See footnote 19.
64 Regulation EU 2022/2554 on digital operational resilience for the financial sector (**DORA**).
65 Articles 7 to 10 DORA.
66 Article 19 DORA.
67 Article 28 DORA.
68 Article 29 DORA.

50 The DORA further requires financial entities to identify, monitor and mitigate *concentration risks* and *vendor lock-in*. Overreliance and dependency on ICT service providers by financial entities (such as CSPs) for critical or important functions may cause significant adverse effects if such ICT services become unavailable or experience failures. Financial entities have to assess carefully whether the use of third-party ICT service providers contributes to or reinforces concentration risks and must weigh the costs and benefits of alternative solutions as well.[69]

51 Under the DORA, management body is responsible for managing the ICT risks of the financial entity,[70] as well as for defining, approving, and overseeing the implementation of the ICT risk management framework.[71] Management body members must actively keep up to date their knowledge and understanding of ICT risks and their impact on the operational side on the financial entity. They must follow regular and specifically tailored trainings to achieve this.[72] It is likely that financial regulators will look at this DORA requirement when assessing the suitability of a proposed board member.[73]

III.2.3 EHDS[74]

52 The EHDS is a proposed regulatory framework aimed at improving natural persons' access to and control over their personal electronic health data. Once adopted, the EDHS will impose rules and procedures for the use and sharing of health data between healthcare institutions in the EU in the context of healthcare services. Under the EHDS, patients will be entitled to free access to their medical documents and information. The EHDS also consolidates the rights of Data Subjects enshrined in the GDPR to broader data categories than personal data. This provides EU patients more access to, control over, and security for their medical data.

53 Furthermore, an EU-wide platform called 'MyHealth@EU' will be established to provide services to support and facilitate the sharing of personal health data between EU healthcare providers.[75] EU member states will need to create national interoperable platforms that allow the exchange of health data through MyHealth@EU.[76]

54 The implementation of the EHDS is without prejudice to the safeguards and obligations from the GDPR and the Data Act, meaning that the processing of health data on the basis of the EHDS must be performed in accordance with the principles and requirements of those acts.[77] The supervisory authorities for the GDPR, Data Act and the EHDS will need to cooperate and facilitate the exercise of rights and the notifications of incidents relating to MyHealth@EU and its national equivalents.[78]

55 Electronic health record systems (**EHR Systems**) provided to EU Entities within scope of the EHDS are subjected to extensive product requirements which must be warranted by manufacturers, importers and distributors of such systems. This means commercial

---

69 Article 29 DORA.
70 Article 5(3)(a) DORA.
71 Article 5(2) DORA.
72 Article 5(4) DORA.
73 Given that Article 2.1.4 DCGC mandates that executives possess the specific expertise necessary for the fulfilment of their role, this is particularly relevant for publicly listed Dutch financial entities.
74 Regulation COM/2022/197 on the European Health Data Space (**EHDS**). The EHDS has recently been approved by the Council of Europe. The regulation will now be formally signed by the Council and the European Parliament. It will enter into force twenty days after publication in the EU's Official Journal. There will be two year implementation period (and longer for certain obligations).
75 Article 23(1) EHDS.
76 Article 23(2) EHDS.
77 Article 1(3) EHDS.
78 Articles 22 and 98(8) EHDS.

(Cloud Service) providers of EHR Systems and EU Entities that use them will have to assess whether their current set-up complies with these product requirements.

IV U.S. LEGAL FRAMEWORK

56 This chapter contains a non-exhaustive list of U.S. laws applicable to U.S. CSPs. These are the CLOUD Act, Section 702 FISA, E.O. 12333 and State Surveillance Laws. Annex II provides a short summary of this chapter per legal act, with the exception of State Surveillance Laws.

IV.1 CLOUD Act

57 The CLOUD Act entered into force on 23 March 2018 and amends the Stored Communications Act by obligating communication service providers established or U.S. to comply with warrants from U.S. Authorities to disclose data in their possession, custody, or control. Such warrants are provided by a U.S. judge if U.S. Authorities reasonably adduce that probable cause exists that the information qualifies as evidence in ongoing (criminal) investigations. What constitutes as 'probable cause' under the CLOUD Act is however not clarified and remains subject to the discretion of U.S. Authorities.

58 The aforementioned obligation applies irrespective of whether the data is located inside or outside the U.S. This means that any communication service provider that is established in the U.S. is subject to compliance with official warrants issued under the CLOUD Act, even when the data is not stored on U.S. soil.

59 CSPs qualify as communication service providers under the CLOUD Act, meaning that EU Entities using Cloud Services provided by CSPs that have a presence in the U.S., must consider the possibility that their data is subject to disclosure with U.S. authorities.

60 U.S. Authorities may request U.S. citizens employed at CSPs outside U.S. jurisdiction to disclose information or provide access to data to which that employee has access, even if that data is located outside the U.S. and without notifying their employer. This may be done voluntarily or by using legal means such as subpoenas. Research has indicated that U.S. employees have the tendency to comply with such requests and provide more data than strictly necessary.[79]

IV.2 Section 702 FISA

61 Section 702 FISA entered into force on 10 July 2008 and allows the U.S. National Security Agency (**NSA**) to collect data stored in the U.S. without a warrant, and of specific non-U.S. citizens reasonably believed to be located outside the U.S.

62 Communication service providers (such as CSPs) can be compelled to allow the surveillance of communications data of non-U.S. citizens. This means that communications data transmitted through the use of Cloud Services and/or stored on data centres used for Public Clouds in the U.S. risk being subjected to an order of disclosure under Section 702 FISA if the CSP providing the Cloud Services falls under the U.S. jurisdiction.

[79] See the advice to the Dutch National Cyber Security Centre dated 26 July 2022 for further references: https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-act-memo.

IV.3 E.O. 12333

63 E.O. 12333 entered into force on 4 December 1981 as a means of strengthening and extending the powers of U.S. Authorities. E.O. 12333 allows for the collection, retention and dissemination of data obtained in the course of 'lawful' foreign intelligence, counterintelligence, international narcotics or international terrorism investigation and 'Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws.' It allows the bulk collection of data in case information necessary to advance a validated intelligence priority cannot "reasonably" be obtained through targeted collection of data.

64 E.O. 12333 has in the past been relied on by the NSA to circumvent the territorial limitation of Section 702 FISA by intercepting data in transit to the U.S. through underwater cables before arriving in the U.S.[80]

IV.4 State Surveillance Laws

65 In addition to the Federal U.S. legal acts discussed above, some U.S. States have adopted State Surveillance Laws.

66 State Surveillance Laws are generally applicable to CSPs in the same way as the CLOUD Act. Broadly speaking, State Surveillance Laws allow (State) U.S. Authorities to serve warrants, subpoenas and court orders to make CSPs disclose data for criminal investigation purposes. Unlike the Federal U.S. laws discussed above, such orders and warrants must be limited to specific data and may only be processed for as specific, pre-identified purpose. An independent court must ultimately examine whether the data requested contains evidence of a crime before granting the warrant, subpoena or court order.

67 The scope and the level of judicial redress available to State Surveillance Laws ultimately varies between individual U.S. States.[81] Although a thorough and individual analysis of State Surveillance Laws goes beyond the scope of this paper, it is pertinent to understand that these laws – in addition to the aforementioned Federal U.S. laws – are included in the broader assessment EU Entities should make when considering engaging a U.S. CSP.

* * *

[80] CJEU 16 July 2020, C-311/18, ECLI:EU:C:2020:559 (*Schrems II*), para 63.
[81] For example, the California Electronic Communications Privacy Act is limited to electronic communication service providers.

Annex I: Overview of key obligations and concerns for Cloud Services in EU law

Laws relating to data protection		
EU law	**Key obligations**	**Key concerns for Cloud Services**
GDPR	• Personal data transfers must comply with the GDPR. • Adequate technical and security measures to prevent personal data leakage	• It is uncertain whether the DPF remains in force for personal data transfers to U.S. CSPs. • Adequate safeguards must be taken to prevent data leakage and loss of control over personal data by EU Entities.
Data Act	• CSPs must take adequate measures to prevent unlawful access to non-personal data by U.S. Authorities. • CSPs must only provide the minimum amount of data in case of a lawful court judgement. • Duty to inform EU entities of a legal order to disclose non-personal data.	• Contractual safeguards between CSPs and EU entities must be included to prevent unlawful access by U.S. Authorities.
Data Governance Act	• CSPs must take adequate measures to prevent unlawful access to non-personal data by U.S. Authorities. • CSPs must only provide the minimum amount of data in case of a lawful court judgement. • Duty to inform EU entities of a legal order to disclose non-personal data.	• Contractual safeguards between CSPs and EU entities must be included to prevent unlawful access by U.S. Authorities.
AI Act	• Special Categories of Personal Data used by high-risk AI system to detect and mitigate bias may not be transferred or accessed by third parties. • A declaration that the high-risk AI system complies with the GDPR is required for a CE-marking.	• U.S. Authorities access may make it impossible to comply with the prohibition to use Special Categories of Personal Data for bias detection in high-risk AI systems. • Transfers of personal data between deployers of high-risk AI systems and CSPs must comply with the GDPR in order to be allowed on the EU market.

Sector-specific laws		
EU law	**Key obligations**	**Key concerns for Cloud Services**
NIS 2	• Duty to report significant incidents by important or essential entities with supervisory authorities. • Implementation of cybersecurity policies, business continuity plans and incident handling practices.	• Deadlines for reporting significant incidents are short and require proactive assistance from U.S. CSPs. • Lack of expertise or knowledge of security measures complicates the drafting of required policies. • Interests for EU Entities and CSPs to comply with NIS 2 are not necessarily aligned.
DORA	• Financial entities must identify, monitor and manage risks and vulnerabilities associated with relying on third-party ICT-service providers for components of their network and information systems. • Duty to report incidents with a high adverse impact on the network and information systems of financial entities. • Financial entities must be aware of CSPs involved in the provision of Cloud Services and contractual warranties must be imposed along the supply chain.	• Deadlines for reporting significant incidents are short and require proactive assistance from U.S. CSPs. • Contracts with U.S. CSPs for Cloud Services supporting critical or important functions may need to be revised to comply with the contractual obligations imposed. • Continuity issues for the durable financial performance of the financial entity may be compromised when a limited pool of (U.S.-based) CSPs provides ICT services to critical or important functions. • Interests for EU Entities and CSPs to comply with the DORA are not necessarily aligned.
EHDS	• GDPR rights for patients in terms of health data that go beyond personal data. • Establishment of EU-wide portal MyHealth@EU for the exchange and sharing of health data. • Imposition of product requirements and interoperability requirements through harmonised software components for EHR systems.	• EU Entities must review their current CSPs used for EHR Systems and check interoperability requirements with harmonised software components imposed. • Cloud Services currently used for EHR Systems may not comply with the product requirements stipulated in the EHDS.

Annex II: Overview of U.S. laws and key EU compliance considerations

US law	Risks for EU Entities	EU compliance consideration
CLOUD Act	• U.S. Authorities can access data stored by U.S CSPs, even if the data is located in another country. • U.S. Authorities can obligate (or request) U.S. citizens to provide information or access to restricted data without informing their employer.	• The possibilities for CSPs to object to warranties of U.S. Authorities regarding EU Data Subjects are limited. • Threshold for allowing access to data by U.S. Authorities is not clearly delineated creating room for interpretation.
Section 702 FISA	• NSA can compel CSPs to allow the surveillance of communications data of non-U.S. citizens.	• DPF may be annulled and current terms and conditions with U.S CSPs may not be suitable afterwards.
E.O. 12333	• Allows U.S. Authorities to collect and intercept bulk data in transit. • Has been used by the NSA to circumvent territorial limit of Section 702 FISA.	• Individual legal redress is limited. E.O. 12333 does not confer enforceable rights to individuals against U.S. Authorities in courts. • DPF may be annulled and current terms and conditions with U.S CSPs may not be suitable afterwards.