UNIVERSITY OF AMSTERDAM

On the Sovereignty of Dutch Government Data

How the National Cloud Policy Falls Short of Protecting Government Data Against Risks From Third Countries' Jurisdiction and Why This Matters

Machiel van der Wal
machielvdwal@gmail.com

Informatierecht

Supervisor: Dr. K. (Kristina) Irion LLM

26 June 2024

Word count: 12992

Abstract

The Dutch government's use of public cloud services from US hyperscalers such as Amazon Web Services is rising. This potentially offers benefits regarding features and cost-efficiency. The question, however, arises whether government data is adequately protected from the jurisdiction of third countries such as the US. In other words, whether government data sovereignty is protected. This concern became especially imminent after the 2022 Dutch national cloud policy, which proved controversial in the scholarly and policy debate. This thesis provides a systematic analysis of how the Dutch legal and policy framework on hosting government data in a public cloud protects the data sovereignty of the Dutch government.

Qualitative research is employed to provide a definition of government data sovereignty based on literature and policy documents. The concept is linked to cybersecurity by defining government data sovereignty as the exclusive authority over government data confidentiality, integrity and availability. Government data sovereignty is conceived as a relative concept which depends on the data's sensitivity. US jurisdiction is identified as a risk to government data sovereignty when data is stored using US hyperscalers or their subsidiaries. This allows the US to compel these cloud service providers via legislation such as the CLOUD Act (law enforcement) and FISA section 702 (intelligence agencies) to hand over customer data, which could be government data. This matters because it would impact the confidentiality of sensitive government data and the state's integrity. This risk cannot always be sufficiently mitigated, and the research shows that a ‘sovereign cloud’ cannot be a business proposition.

Evaluative legal research shows that the Dutch legal and policy framework for hosting government data in the cloud takes a risk-based approach. State secrets cannot be stored in a public cloud. This effectively guarantees data sovereignty for state secrets. A risk assessment should be made for all other types of government data. The prescribed risk assessment includes criteria relevant to data sovereignty, potentially offering protection. However, it is unclear how the risk to government data sovereignty should be weighed compared to, for example, the benefits of self-hosted solutions. A way to better protect government data sovereignty could be introducing data sovereignty requirements for additional sensitive data types. This would require the Netherlands to deviate from the current market-oriented risk-based approach, which, as this research shows, is also apparent in its stance in the European Cloud Certification Scheme discussion.

Table of contents

List of abbreviations

ACM	Autoriteit Consument en Markt
AWS	Amazon Web Services
EUCS	European Cybersecurity Certification Scheme for Cloud Services
EU	European Union
US	United States
IaaS	Infrastructure as a Service
MLAT	Mutual Legal Assistance Treaties
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
SaaS	Software as a Service

1. Introduction

Dutch society is highly digitised - the Netherlands ranks third in the European Union's Digital Economy and Society Index.[1] The Dutch government is highly digitised as well.[2] The tax authority, for example, uses almost 900 different applications (a type of software providing digital functionality for an end-user).[3] The Rijksoverheid (Dutch central government) provides almost 1800 different websites.[4] This digitalization of government results in a lot of government data of different sensitivities, ranging from public information on government websites to top secret state secrets.

Governments can store their data on their own servers, but a shift to the use of cloud services for data storage has been observed in the last decade.[5] Cloud computing is often used to describe the model for "on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services storage) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[6] Cloud computing is offered as a service in various forms. Data storage via such a service has various advantages compared to traditional self-hosting, such as higher cost efficiency and easy scalability.[7] Various security concerns exist depending on the type of cloud storage service,[8] but the security offered by the cloud service provider could be higher than the traditional self-hosting hosting due to scale and security budget advantages.[9] However, cloud storage also poses risks, such as possible *lock-in* effects[10] and the risk of exposing data to the jurisdiction of foreign countries, which is also a security risk. The majority of the Dutch cloud market (75-90%) is in the hands of only three cloud service

[1] European Commission 2022.

[2] Demirel, Koens & Vennekens 2023.

[3] *Kamerstukken II 2018/19*, 31066, nr. 486, p. 2.

[4] 'Websiteregister Rijksoverheid', communicatierijk.nl, april 2024.

[5] ACM 2022, p. 7; Gürses & Van Hoboken 2018, p. 583-586.

[6] NIST 2011, p. 2.

[7] Tweneboa-Koduah, Endicott-Popovsky & Tsetse 2014, p. 2–4.

[8] Ali, Khan & Vasilakos 2015, p. 360–365; Alouffi et al. 2021, p. 57798-57805.

[9] Blancato 2023, p. 15.

[10] ACM 2022, p. 59–65.

providers, so-called hyper scalers, namely Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform.[11]

In the last decade, the Dutch government[12] hosted its data in a private cloud, storing it in its own data centres in the Netherlands, the so-called ‘closed Rijkscloud’.[13] That policy originated in 2011, when the Dutch government argued that the risks of using a public cloud service outweighed the potential benefits.[14] In 2022, the government introduced their new ‘Rijksbreed cloudbeleid’ (national cloud policy), allowing central government organizations to use public cloud services for more data types.[15] The government's use of these cloud services has risen since then. In 2022, more than 50% of the software applications tendered by the Dutch government concerned a form of cloud services.[16]

The new Dutch cloud policy raised controversy among legal scholars,[17] parliamentarians,[18] and in broader policy discussions on the Dutch[19] and EU level.[20] The second chamber adopted a motion calling the government to reconsider transferring government data outside the European Economic Area (EEA) and choose a European cloud service provider.[21] The critique focuses, for a large part, on the risk of government data being under a foreign jurisdiction, either because the data is hosted in a foreign country or because of the cloud service provider’s nexus with a third country. The concept of government (or national) data sovereignty can be used to highlight the risks of placing government data in the cloud and, thereby, under a foreign jurisdiction.

On the EU level, a discussion on data sovereignty is taking place surrounding the European Cybersecurity Certification Scheme for Cloud Services (EUCS) that was proposed

[11] ACM 2022, p. 34-37.

[12] Unless specified otherwise, ‘Dutch government’ will be used to refer to the Rijksoverheid.

[13] *Kamerstukken II* 2010/11*,* 26643, nr. 179, p. 3.

[14] *Kamerstukken II* 2010/11*,* 26643, nr. 179, p. 3.

[15] Letter from the state secretary of the interior and kingdom relations of 29 August 2022 (*Kamerstukken II* 2021/22, 26643, nr. 904).

[16] ICTU 2024, p. 16–18.

[17] Krikke 2022; Van Dijck & Jacobs 2022; Hartholt 2022.

[18] *Kamerstukken II* 2022/23, 26643, nr. 963.

[19] Gomes & Okano-Heijmans 2024.

[20] Gkritsi 2024.

[21] *Kamerstukken II* 2022/23, 26643, nr. 975.

by the European Union Agency for Cyber Security (ENISA) in 2020 based on the Cybersecurity Act.[22] Data sovereignty requirements were included in subsequent drafts after pressure from several member states, primarily France.[23] These drafts required companies offering certain types of services with a need for the highest security standards to be immune from foreign law and process data solely within the EU.[24] The certification scheme is still being heavily discussed. Although certification is voluntary based on the Cybersecurity Act, they could legally be made mandatory under the NIS 2 Directive for certain entities by the European Commission or Member States.[25] Governments could also require such a certification in public procurement, making them de facto mandatory.

Irion was the first to analyze the concept of data sovereignty in relation to government data in the literature in 2012.[26] Data sovereignty means different things depending on the context and is not an established legal concept.[27] She argues that data sovereignty is "a crucial dimension of national sovereignty that presupposes the nation state".[28] National data sovereignty is defined as "Government's exclusive authority and control over all virtual public assets, which are not in the public domain, irrespective of whether they are stored on their own or third parties' facilities and premises".[29] She subsequently analyses the cloud computing strategies in Australia, Canada, the United Kingdom, and the US to assess how these countries protect national data sovereignty. Her conclusion is that data sovereignty risks cannot be fully addressed by contractual arrangements or technology and that additional strategies are used.[30]

According to a systematic literature review of Hummel et al. in 2021, the concept of data sovereignty is still used in various ways and with various connotations in the literature,

[22] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (*OJ* 2019, L 151/15).

[23] Prop 2022.

[24] Prop 2022.

[25] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (*OJ* 2022, L 333), art. 21.

[26] Irion 2012, p. 42.

[27] Irion 2012, p. 50.

[28] Irion 2012, p. 42.

[29] Irion 2012, p. 41.

[30] Irion 2012, p. 59.

depending on the context.[31] Clarity on the definition of data sovereignty that is adopted can help reflect on the concept's nature and allows for concrete discussion on what is needed to achieve it.[32]

Hildén draws upon Irions definition of national data sovereignty and discusses the legal risk of using US cloud services, resulting in EU public sector data being under US jurisdiction.[33] He focuses mainly on government data which is also personal data. The use of Microsoft Office by the Dutch government and the associated negotiations is used as a case study.[34] Blancato discusses data sovereignty in relation to the EU regulatory approach to the cloud sector, US cloud service providers and the CLOUD Act.[35] His article furthermore draws a link between data sovereignty and the EU trying to "revive the competitiveness of the European industrial ecosystem in digital technologies", which is part of a broader strategic goal.[36]

Regarding the Dutch context, Krikke criticizes the new national cloud policy.[37] She argues that the risk assessment that is introduced in the policy is mainly focused on personal data and less on other sensitive government data.[38] She does not connect the policy to the concept of data sovereignty. Weij raises the question of whether we should just accept the risks associated with placing government data under a foreign jurisdiction.[39] Commissioned by the Dutch intelligence agency AIVD, Gomes & Okano-Heijmans briefly analyse the cloud policy in relation to 'cloud sovereignty', of which data sovereignty is a part in their view.[40]

Based on the literature review above, the research gap addressed by this thesis is a lack of a systematic analysis of how the Dutch legal and policy framework on hosting government data in a public cloud protects the data sovereignty of the Dutch government and whether this suffices, especially concerning non-personal government data. Its broader relevance lies in

[31] Hummel et al. 2021, p. 12; Irion 2012, p. 50.

[32] Hummel et al. 2021, p. 13-14.

[33] Hildén 2021.

[34] Hildén 2021, p. 11-13.

[35] Blancato 2023.

[36] Blancato 2023, p. 13.

[37] Krikke 2022.

[38] Krikke 2022, p. 188.

[39] Weij 2024, p. 78.

[40] Gomes & Okano-Heijmans 2024, p. 5.

the research's contribution to the ongoing and growing political and policy discussions on the Dutch government's current use of cloud services and the data sovereignty risks.[41]

1.1 Research question

The following main research question will be addressed: *How does the Dutch legal and policy framework on hosting government data in a public cloud protect Dutch government data sovereignty, and why does this matter?*

This question will be answered by the following subquestions:

1. *What is government data sovereignty?*
2. *What is the Dutch legal and policy framework for hosting Dutch government data in a public cloud?*
3. *Is data sovereignty protected in the Dutch legal and policy framework and, if so, how?*

The focus of the research will be mainly on non-personal Dutch government data. The definition of government data sovereignty will be provided in section 2.1. Public cloud follows the influential definition of the National Institute of Standards and Technology (NIST).[42] Hosting is defined as the storage of data in a public cloud. Data and information are used interchangeably in this thesis. The Dutch legal and policy framework is seen as the BIO,[43] VIRBI 2013,[44] VIR,[45] the national cloud policy and the associated risk assessment framework.[46] These all apply to the storage of government data. The influence of the NIS 2 Directive concerning the duty of care and the influence of the Cybersecurity Act, specifically the EUCS, is seen as relevant for this Dutch legal and policy framework. The GDPR is briefly included when personal data is considered to be able to provide an overview of the

[41] Rensen 2024; Hubert 2024; 'Plenair debat over uitbesteding ICT aan Amerikaanse techbedrijven gaat er komen', ibestuur.nl, 7 juni 2024.

[42] NIST 2011; NIST 2018.

[43] Circulaire van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van 11 februari 2020 inzake het toepassen van de Baseline Informatiebeveiliging Overheid [BIO] in het digitale verkeer met het Rijk (*Stcrt.* 2020, 7857).

[44] Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (*Stcrt.* 2013, 154970).

[45] Besluit voorschrift informatiebeveiliging rijksdienst 2007 (*Stcrt.* 2007, 122).

[46] Letter from the state secretary of the interior and kingdom relations of 24 January 2023 (Appendix with *Kamerstukken II* 2022/23, 26643, nr. 963).

framework. Due to the limited size of the thesis, other laws governing more specific types of government data, such as the Archive law[47], and public procurement law are out of scope.

1.1 Methodology

This research will evaluate the Dutch legal and policy framework for storing data in a public cloud based on the external normative criterion of government data sovereignty. This criterion is external because it is not derived from the legal system itself.[48] Mixed research methods will, therefore, be used to answer the main evaluative research question, compared to merely traditional legal research.[49]

Qualitative research will be employed by analysing Dutch and English policy documents and literature to answer the first descriptive subquestion. Policy documents on the EU and the Dutch level are included to show that government data sovereignty is a policy aim, which renders it suitable as a standard as a building block for an external normative framework.[50] Forward snowballing is used to select relevant literature on government data sovereignty, starting with Irion's article on national data sovereignty[51] and the systematic literature review on ‘data sovereignty’ by Hummel et al.[52] From there, a combination of forward and backward snowballing is used. The advantage of this methodology is that relevant articles are more easily found because the data collection starts with two relevant articles.[53] The data collection is supplemented by a search in Kluwer Inview, Legal Intelligence, Google Scholar and WorldCat Discovery with i.a. the search terms “data sovereignty AND government”, “US CLOUD Act”, “government AND cloud”, “Rijksbreed cloudbeleid”, “Dutch cloud policy”. Legal literature is included to describe the application of extra-territorial jurisdiction to government data. Information systems literature is included to describe the different types of cloud services and their (dis)advantages. The normative criterion is further operationalized by relating it to the concept of cybersecurity.

[47] Archiefwet 1995 (*Stb.* 1995, 276).

[48] Kestemont 2015, p. 374, 376.

[49] Kestemont 2015, p. 374. Traditional legal research is seen as legal doctrinal research, see e.g. Tjong Tjin Tai & Paul Verbruggen 2022, p. 4-5.

[50] Taekema 2018, p. 8-9.

[51] Irion 2012.

[52] Hummel et al. 2021.

[53] Wohlin 2015, p. 9.

The second descriptive research question is answered by employing legal doctrinal research. This method will provide a systematic description of the applicable laws and policies.[54] The selection of laws and policies that will be analysed is provided in section 1.1. Next to this, relevant explanatory memorandums and parliamentary debates are included to further describe and explain the framework. An overview of the included documents is provided in the bibliography.

The third subquestion will be answered by employing evaluative legal research on how data sovereignty is protected by the legal and policy framework and whether it suffices.[55] This will be done by analysing the answer to the second research question through the lens of government data sovereignty as described and operationalized by the answer to the first subquestion.[56] The discussion on the EUCS will be included in the evaluation to provide more context on the Dutch rationales for the framework. This is mainly derived from Euractiv news articles. The result will be an analysis of how government data sovereignty is protected in the Dutch legal and policy framework.

1.2 Structure

The structure of this research is as follows. Chapter 2 will first discuss and define the concept of government data sovereignty in policy and literature. Then, a description of cloud services and the cloud market is provided, highlighting the relationship between government data sovereignty and the government's use of public cloud services. The risk to government data sovereignty is further contextualized by discussing US legislation claiming extra-territorial jurisdiction. Chapter 3 will describe the Dutch legal and policy framework for storing government data in the public cloud. First, the influence of EU legislation is described. Then, the Dutch framework is identified, showing a risk-based approach. Chapter 4 will analyse the Dutch legal and policy framework through the lens of protecting government data sovereignty. In this chapter, the discussion on the EUCS will be highlighted to describe the concept of data sovereignty requirements and the arguments for and against it. The research will end with a conclusion in Chapter 5.

[54] Tjong Tjin Tai & Verbruggen 2022, p. 4-5; Snel & Vranken, p. 714.

[55] Kestemont 2015, p. 373-375.

[56] Kestemont 2015, p. 373.

2 Government data sovereignty and the cloud

In this chapter, the concept of data sovereignty will be set out based on policy documents and literature. Then, the use of cloud services will be discussed in light of the effect it could have on data sovereignty. Next, the Dutch and European cloud market is identified, showing three US hyperscalers dominating this, with lock-in effects occurring. Lastly, US extra-territorial jurisdiction is discussed together with FISA section 702 and the CLOUD Act as examples of legislation impacting government data sovereignty.

2.1 Government Data Sovereignty

2.1.1 Policy

Data sovereignty is a part of both the EU and the Dutch policy agenda, although the concept is often not mentioned as such or not clearly defined.[57] On the European level, the risk of data being subject to the jurisdiction of a third country was already mentioned in the European strategy for data in 2020, together with 'technological sovereignty'.[58] Control over data is seen as essential for digital sovereignty by the Commissioner for the Internal Market, Thierry Breton.[59] Data sovereignty can be seen as a part of digital sovereignty.

Data sovereignty is also part of the Dutch 'Digital Open Strategic Autonomy' policy agenda. The government will start investigating possible mitigation measures to decrease Dutch dependency on foreign cloud providers and the feasibility of a 'sovereign Dutch cloud' in the future as part of this.[60] The Algemene Rekenkamer (a Dutch supervisory authority) recently started investigating sovereignty and data related to cloud services.[61]

2.1.2 Literature

Government data sovereignty is not (yet) an established legal concept and consequently has no clear legal definition.[62] In the literature, the concept of data sovereignty is used to describe

[57] Michels, Millard & Walden 2023, p. 14.

[58] European Commission 2020, p. 9-10.

[59] Breton 2022.

[60] Appendix with *Kamerstukken II* 2023/24, 36259, nr. 21, p. 26.

[61] 'Het Rijk in de cloud', rekenkamer.nl.

[62] Irion 2012, p. 50; *Kamerstukken II* 2018/19, 33694 26643, nr. 47.

various notions and issues, depending on the context.[63] Generally speaking, it describes preserving governments' exclusive jurisdiction and control over data.[64] As such, it clearly draws from the traditional definition of territorial sovereignty, which is the exclusive right of the state to exercise the functions of a state inside of its territory.[65] Irion argues that data sovereignty is a dimension of national sovereignty and a function of the nation state.[66] Other authors argue that a form of data sovereignty can be grounded in the concept of State dignity.[67]

The extent of government data sovereignty cannot fully be captured with existing rights and legislation. Since information and data are intangible, property rights do not apply to this as such (only to the carriers, such as servers) and, therefore, can not be exercised.[68] Personal data protection laws apply to personal data, but not all (sensitive) data is personal data, e.g. state secrets on the condition of critical infrastructure.

For this thesis, the following working definition of data sovereignty is adopted: "Government's exclusive authority [….] over all virtual public assets, which are not in the public domain, irrespective of whether they are stored on their own or third parties' facilities and premises".[69] Data sovereignty is often understood as a relative concept.[70] The approach to maintaining data sovereignty then depends on the sensitivity of the public asset, i.e. data, involved.

2.1.3 Government data sovereignty and cybersecurity

A relative, often risk-based approach to data sovereignty can be seen as a logical consequence of the relationship between data sovereignty and cybersecurity.[71] Cybersecurity refers to protecting the confidentiality, integrity and availability[72] of information (and systems).

[63] Hummel et al. 2021, p. 8.

[64] Michels, Millard & Walden 2023, p. 14; Irion 2012, p. 42, 65.

[65] Svantesson et al. 2023, p. 39; Michels, Millard & Walden 2023, p. 11-12.

[66] Irion 2012, p. 65.

[67] For a version of this argument, see Svantesson et al. 2023.

[68] Michels & Millard 2022, p. 324-329.

[69] Irion 2012, p. 41.

[70] Irion 2012, p. 66.

[71] Michels, Millard & Walden 2023, p. 19-20; Irion 2012, p. 50-51.

[72] Often abbreviated as CIA.

Cybersecurity measures often involve a risk-based approach in which the type of information is defined first. Secondly, the associated risks are assessed, and lastly, mitigating measures appropriate to the risks are determined. This is an ongoing process because the risks can change due to changing circumstances.

Compare, for example, information on a public government website to state secrets. For the public information on a government website, confidentiality is not at risk (it is already public), but integrity (the correctness of the information) could still be important, as is the availability to the public. For state secrets, confidentiality is of the utmost importance. Therefore, the related mitigating measures should differ for these two types of government information.

Because government data sovereignty concerns virtual *public* assets, any reduction of authority over data could have effects reaching beyond compromising the government data itself. It could have implications for the functioning of the state itself. Irion states, "The ability to govern presupposes command and control over government information to the extent necessary to deliver public services and public goods as well as to ensure the integrity of the state".[73] These second-order effects should lead to a different risk assessment for governments than cybersecurity assessments for, e.g. companies. The next section will show the potential risk to data sovereignty due to the use of cloud services.

2.2 Cloud services

Cloud computing is often defined following the definition of the US National Institute of Standards and Technology (NIST) as: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[74] This definition has influenced EU legislation, e.g. the NIS 2 Directive,[75] and the Dutch cloud policy, which refers to the NIST definition.[76]

[73] Irion 2012, p. 53.

[74] NIST 2011, p. 2; NIST 2018, p. 2.

[75] Art. 6(1)(30) NIS 2 Directive, where 'cloud computing service' is defined as "a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations".

[76] National cloud policy, p. 6-7.

2.2.1 Characteristics

Five essential characteristics of cloud computing can be distinguished, which can be directly related to its benefits and risks. Those are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.[77] On-demand self-service refers to the ability of the cloud service customer to request computing capabilities, such as storage, unilaterally.[78] Broad network access means that the computing capability can be accessed from different locations via a network, such as the internet.[79] Resource pooling refers to the fact that computing resources are pooled. This means that they are shared between more than one cloud service customer.[80] Those resources are dynamically assigned by the cloud service provider based on demand. Apart from this, “there is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resource, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter).”[81] Rapid elasticity refers to the fact that computing capabilities can rapidly be provided to the cloud service customer based on demand, for example, when extra storage space is needed.[82] Lastly, measured service refers to the ability of the cloud service to “control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, […])” while providing transparency to both the cloud service customer and the cloud service provider of the utilized service.[83]

2.2.2 Advantages and disadvantages

These characteristics of cloud computing come with potential benefits. The scalability allows for flexibility and higher cost efficiency.[84] This results from the computing resources being provided on a pay-for-use basis. Using cloud services shifts the costs from capital expenditures (i.e. buying your own servers) to operational expenditures (i.e. paying for a

[77] NIST 2018, p. 4-8.

[78] NIST 2018, p. 4.

[79] NIST 2018, p. 5.

[80] NIST 2018, p. 6.

[81] NIST 2018, p. 5-6.

[82] NIST 2018, p. 7.

[83] NIST 2018, p. 7-8.

[84] Tweneboa-Koduah, Endicott-Popovsky & Tsetse 2014, p. 2–4.

cloud storage service).[85] Cloud services can have a security advantage due to resource pooling, when e.g. data is stored in multiple data centres, by offering redundancy and resilience.[86] This contributes to the availability of the data. Further security benefits can exist depending on the cloud service provider due to the benefits of scale resulting from the resource pooling.

However, there are also various (technical) security risks with the use of cloud computing.[87] Only recently have hackers associated with China accessed the official email accounts of senior US government officials managing US-China relations.[88] The independent US Cyber Safety Review Board concluded that "Microsoft's security culture was inadequate" and that Microsoft made a "cascade of […] avoidable errors that allowed this intrusion to succeed".[89] This example illustrates that using cloud services is not necessarily more secure but that the customer becomes dependent on the measures taken by the provider. These might prove insufficient.

2.2.3 The risk to government data sovereignty

Storing government data in the cloud potentially threatens government data security. This results from dependency on the cloud service provider and concurrent jurisdiction and, thus, form a risk to government data sovereignty. According to Bigo et. al, "once data is transferred into a Cloud, sovereignty is surrendered".[90]

Two situations should be distinguished in this regard. The first situation is that the data is being hosted in a foreign country, which is why the foreign jurisdiction applies based on territoriality. The second situation is when data is hosted domestically or in another EU Member State, but a foreign jurisdiction applies by virtue of the cloud service provider's nexus with a third country. An example of this is hosting data via AWS in Europe, while the

[85] Blancato 2023, p. 15.

[86] Blancato 2023, p. 15.

[87] Ali, Khan & Vasilakos 2015, p. 360–365; Alouffi et al. 2021, p. 57798-57805.

[88] Cyber Safety Review Board 2024, p. ii-iii.

[89] Cyber Security Review Board 2024, p. 17. See also Dudley & Burke 2024.

[90] Bigo et al. 2012, p. 35.

US claims jurisdiction over the cloud service provider based on their Clarifying Lawful Overseas Use of Data Act (CLOUD Act).[91] Section 2.4 will elaborate on this.

To address the first situation, Microsoft,[92] AWS,[93] and Google[94] introduced a 'sovereign cloud' as a business proposition.[95] This can be seen as a localised cloud service, where data transfers outside of the EU are minimized. This data localisation should, therefore, prevent concurrent jurisdictions from applying based on territoriality. Data is stored in a network of data centres in Europe instead of in a worldwide network of data centres worldwide.[96] This type of data localization often does not apply to all metadata, which is data about the content data (when it is accessed and by whom, the type of data, etc.), for e.g. security reasons.[97] Therefore, that type of data could still become subject to a jurisdiction based on territoriality and could form a risk to data sovereignty. Data localisation does not address the second situation, in which jurisdiction is claimed via a nexus of the cloud service provider with a foreign jurisdiction, which will be elaborated on in section 2.3. The contract with the cloud service provider would not be able to mitigate that risk because a contract only binds the parties to the contract and does not prevent cloud service providers from complying with the applying jurisdictions' legal obligations.[98]

2.2.4 Cloud service models

It has been established that cloud (data) storage is a form of cloud computing. Cloud computing is seen as a service model, in which three main types are distinguished: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).[99] This 'as a Service' suffix emphasises the fact that computing resources are rented from a service provider instead of owned and run by the customer.[100] Data storage is part of the

[91] Clarifying Lawful Overseas Use of Data Act 2018, H.R. 4943.

[92] Microsoft 2022.

[93] Hugo 2024; Amazon 2023.

[94] Google 2022.

[95] Blancato 2023, p. 22.

[96] Michels, Miljard & Walden 2023, p. 8.

[97] Michels, Miljard & Walden 2023, p. 9-10.

[98] Irion 2012, p. 51.

[99] NIST 2018, p. 9-11.

[100] Hon, Millard & Singh 2022a, p. 7.

service with all SaaS, PaaS and IaaS. Going for a greater to a lesser level of abstraction,[101] SaaS offers end-user applications, such as Microsoft Office 365, for online word processing. PaaS is an offering of a platform on which applications can be developed by the cloud service customer itself. IaaS is an offering of just the computing resources, such as storage.[102] This shows the dependency of the cloud service customer on the cloud service provider for the provisioning of storage and the security of the data stored.

2.2.5 Cloud deployment models

To further differentiate between different cloud service offerings, four types of deployment models can be distinguished: private cloud, community cloud, public cloud and hybrid cloud.[103] With a private cloud, the infrastructure of computing resources is provided by a single organisation for a single organisation or related entities. An example is the 'Rijkscloud', managed by a Dutch government organisation for eight Dutch ministries.[104] private cloud can both be on-premise and off-premise. A community cloud provides the infrastructure for a specific group of customers with aligned interests, such as financial institutions.[105] A public cloud concerns infrastructure provided "for open use by the general public".[106] A hybrid cloud combines two or more of the aforementioned infrastructures.[107]

2.2.6 The cloud market

The Dutch and the EU cloud markets are dominated by three large US cloud providers, also called hyperscalers.[108] According to a market study of the Dutch Autoriteit Consument en Markt (ACM), Microsoft Azure holds 40-45% of the Dutch market shares, AWS 30-35% and Google Cloud Platform 5-10%.[109] The Microsoft Azure market share in the Netherlands is considerably bigger than its share in the EU market (35-40%) because the Netherlands is

[101] Blancato 2023, p. 15.

[102] Hon, Millard & Singh 2022a, p. 7-21; NIST 2011, p. 2-3.

[103] NIST 2018, p. 12.

[104] 'Overheidsdatacenter Noord', odc-noord.nl; *Kamerstukken II* 2010/11*,* 26643, nr. 179, p. 3.

[105] Hon, Millard & Singh 2022a, p. 9.

[106] NIST 2018, p. 12.

[107] NIST 2018, p. 12.

[108] ACM 2022, p. 37.

[109] ACM 2022, p. 37.

"relatively a Microsoft-oriented country".[110] These three hyperscalers are also mostly used by the Dutch government,[111] which established a separate department within the Ministerie voor Justitie en Veiligheid for initiating government-wide service-level agreements.[112]

According to the ACM, an important characteristic of the current cloud market is the risk of a lock-in effect.[113] This effect occurs when migrating from one cloud provider to another is costly. They observe that a choice for a certain cloud provider is most often a one-time choice for enterprise customers. The costs result from customers modifying their organizational processes to the offered cloud services. Switching to another cloud service would also cost time and effort to change these processes. A more direct cost could exist in egress fees, which are fees the cloud service provider charges to move data from one cloud service to another. This depends on the contractual agreement.

2.3 Extra-territorial jurisdiction and government data sovereignty

Because of the dominance of and dependency on US hyperscalers in the Dutch cloud market, data sovereignty concerns mainly relate to the dependency on US cloud service providers combined with US legislation claiming extra-territorial jurisdiction. Several other countries have introduced legislation to compel service providers to disclose data regardless of the storage location of the data, e.g. Australia and China.[114] These are, however, out of the scope of this thesis.

In the case of the US, two types of powers can be distinguished.[115] The first is law intelligence agencies obtaining data for national security reasons (e.g. via FISA section 702), and the second is law enforcement agencies obtaining data for reasons of public security (e.g. via the CLOUD Act).

Based on FISA section 702, intelligence services can compel cloud service providers to provide foreign intelligence information, with the obligation to not provide any

[110] ACM 2022, p. 37; see also Hubert 2024.

[111] ACM 2022, p. 29.

[112] 'Over SLM Microsoft, Google Cloud en Amazon Web Services', slmmicrosoftrijk.nl.

[113] ACM 2022, p. 57; See also Appendix with *Kamerstukken II* 2023/24, 36259, nr. 21, p. 24.

[114] NSCS 2022.

[115] Michels, Millard & Walden 2023, p. 27.

information on this to the cloud service consumer.[116] Foreign intelligence information is defined as information that can help the US protect itself from, e.g. terrorist attacks and information related to "the national defense or the security" and "the conduct of the foreign affairs" of the US.[117] Many types of (sensitive) government data could thus be in the scope of this definition. The US intelligence community is very much aware of the advantage it has via US companies such as cloud service providers. The President's Intelligence Advisory Board stated in an evaluation of FISA section 702: "As a world leader in telecommunications, U.S. telecommunications services are ubiquitous, and the intelligence community can leverage this national advantage to collect foreign intelligence information by lawful, court-approved methods to protect America from its adversaries and support foreign policy decisions that help advance America's standing in the world."[118]

The Clarifying Lawful Overseas Use of Data Act (CLOUD Act), amending i.a. the Stored Communications Act,[119] is another often-cited example of a US federal law impacting (data) sovereignty of other countries.[120] It requires that a service provider discloses data, regardless of the location, to US law enforcement agencies based on a warrant.

As a "longstanding US principle", any foreign company with sufficient contacts with the US is subject to US jurisdiction (the 'minimum contacts test'), next to US legal entities and foreign entities with e.g. a branch office in the US.[121] The test for personal jurisdiction that is used by US courts takes into account the nature, quantity and quality of these contacts.[122] Relevant is, i.a., whether the company markets or sells products or services in the US and whether it uses US-based servers when it offers services online, such as a cloud service provider.[123] Because of this principle, the US at least claims jurisdiction over US cloud service providers and any subsidiaries offering cloud services in Europe, regardless of where the data is stored.

[116] 50 U.S.C. § 1801a(i)

[117] 50 U.S.C. § 1801(e).

[118] PIAB & IOB 2023, p. 3.

[119] 18 U.S.C § 2713.

[120] Blancato 2023, p. 20-22; Michel, Millard & Walden 2023, p. 27-28; Walden 2021, p. 442; Hildén 2021, p. 4-6; Abraha 2020, p. 332.

[121] Abraha 2020, p. 336; Mignon 2020, p. 113; Greenberg Traurig 2022a, p. 3-8;

[122] Abraha 2020, p. 336.

[123] Greenberg Traurig 2022a, p. 3.

The next section serves as one example to illustrate how the US compels cloud service providers to disclose data by claiming jurisdiction, thereby posing a threat to government data sovereignty.

2.3.1 The US CLOUD Act

Paragraph 2713 in chapter 121 of Title 18 of the United States Code states:

> "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States".[124]

The CLOUD Act takes a "geography agnostic approach to jurisdiction over cloud data" and focuses on the service provider to claim jurisdiction over data in the cloud.[125] As such, this law bypasses mutual legal assistance treaties (MLAT), which is the standard international process for data sharing between law enforcement agencies upon request, because they are deemed too slow.[126] Where it concerns personal data, EU data protection regulators argued that this MLAT circumvention interferes with the "territorial sovereignty of an EU member state".[127]

Cloud computing services are seen as remote computing services, which, i.a., cover the provision of computer storage.[128] The US government may only issue a warrant when there is probable cause that the requested data will contain evidence of a crime, which provides a safeguard in itself.[129] However, the CLOUD Act also establishes a framework on the basis of which other governments can, after reaching an agreement with the US, access the same data without using the standard MLAT process.[130] A lower standard than 'probable

[124] 18 U.S.C § 2713, emphasis added.

[125] Abraha 2020, p. 332-336.

[126] Blancato 2023, p. 20; Propp 2022.

[127] Article 29 Working Party 2017, p. 9. Such transfers are outlawed by art. 48 GDPR.

[128] 18 U.S.C § 2711(2).

[129] Greenberg Traurig 2022a, p. 2-3; see 18 U.S.C. § 2703(d).

[130] 18 U.S.C. § 2523; Abraha 2020, p. 340-341.

cause' applies for those orders, namely the requirement that the order is "based on requirements for a reasonable justification based on articulable and credible facts".[131] It could be said that this accommodates the different process standards in various countries, but it provides less protection than the US 'probable cause' standard.[132]

The CLOUD Act does not define what 'possession, custody, or control' entails, but it does not require providers to be able to decrypt the data that they store.[133] Therefore, encryption could form a safeguard against the CLOUD Act and protect the confidentiality of data by technical means, thereby maintaining data sovereignty; encryption, or two-way cryptography, is a method to transform data into a code without meaning. The code can only be transformed back to the original data by whoever has the unique decryption key. The strength of the encryption depends on i.a. the encryption method, the length of the unique key and the way the unique key is stored.[134] It varies whether the cloud service provider has access to the key, which could allow them to fulfil the 'possession, custody, or control' criterion. Many SaaS applications require the cloud service provider to possess the key, while this is not the case for PaaS and IaaS.[135] Furthermore, the cloud provider will be the party implementing the encryption. When the US claims jurisdiction over this provider, the risk of the US compelling the provider to undo these measures still cannot fully be mitigated.

2.3.2 The risk in practice

The CLOUD Act and similar legislation, such as FISA section 702, can thus pose a risk to data sovereignty because the US claims jurisdiction over cloud service providers with a connection to the US. They can force them to disclose information over which they have control, also when this is government data stored by such a provider. It, therefore, forms a direct risk to the confidentiality of this data.

It is a separate question whether this risk materialises in practice. The NCSC mandated a separate report on this question, with the conclusion that this risk is very low.[136] This report was based on transparency reports from hyperscalers. Between January 2018 and

[131] 18 U.S.C. § 2523(b)(4)(D)(iv).

[132] Abraha 2020, p. 347-348.

[133] Greenberg Traurig 2022a, p. 3.

[134] Hon, Millard & Singh 2022b, p. 13.

[135] Hon, Millard & Singh 2022b, p. 5, 15-16.

[136] Greenberg Traurig 2022b.

June 2022, Microsoft disclosed the content data of non-US enterprise customers twelve times.[137] Between July and December 2022, this number increased to sixteen, with 62 CLOUD Act warrants in that timeframe.[138] It increased to twenty in the first half of 2023, with 58 warrants.[139] Although the chance of the risk materialising seems to be low, there is no information on the type of enterprise customer targeted and the sensitivity of the data disclosed. Furthermore, the risk of the US being interested in the government data of its allies, such as The Netherlands, is not imaginary. In the last two decades, the NSA has e.g. gathered intelligence from the German Chancellery and French ministers.[140]

The US personal jurisdiction principle also creates a risk to data sovereignty via the availability of data when the US government orders a US cloud service provider to stop providing its services to the government. Although the risk of this happening is low, it still would impact government data sovereignty. The fact that the data would be stored in the EU in a ‘sovereign cloud’ would not change this.

2.4 Subconclusion

This chapter defined the concept of government data sovereignty as governments having exclusive authority over their data. It is related to cybersecurity and concerns the authority over government data's confidentiality, integrity and availability. It is viewed as a relative concept, meaning that different standards can apply to different data types. Concurrent jurisdiction poses a risk to primarily the confidentiality of data and, thereby, to data sovereignty. This risk can form when a government uses cloud services from a cloud service provider which is subject to a foreign jurisdiction. Data sovereignty cannot be a business proposition because contractual agreements between the service provider and the government do not work externally. As a result of US hyperscalers dominating the European and Dutch cloud market, the risk is pertinent. The US claims jurisdiction over US companies, any subsidiaries and any other companies with sufficient contact with the US. Via the US CLOUD Act and FISA 702, the US compels cloud service providers to disclose information, regardless of whether they are established on US territory. Furthermore, it prohibits them

[137] Geenberg Traurig 2022b, p. 5.

[138] Microsoft 2024.

[139] Microsoft 2024.

[140] The Guardian 2015.

from disclosing this to the cloud service customer. Although encryption can provide a safeguard, this possibility depends on the specific cloud service. The amount of US CLOUD Act requests complied with by cloud service providers is low, but there is no information on the exact nature of disclosed data. Either way, the CLOUD Act and similar legislation impact government data sovereignty when using US public cloud services.

3. The Dutch approach to government data and the public cloud

This chapter will elaborate on the Dutch government's legal and policy framework for hosting Dutch government data in a public cloud. First, the influence of EU legislation, namely the NIS 2 Directive and the Cybersecurity Act, will be discussed. Thereafter, the Dutch legal and policy framework for storing Dutch government data in a public cloud will be discussed. This framework comprises BIO, VIR, VIRBI 2013, the national cloud policy and the accompanying risk assessment framework.

3.1 Influence of EU legislation

3.1.1 The NIS 2 Directive

The aim of the NIS 2 Directive is "to achieve a high common level of cybersecurity across the Union".[141] It is a form of EU law which applies in the Dutch legal system when it is transposed.[142] The directive is a successor to the NIS Directive,[143] which was implemented in the Dutch law on the protection of network and information systems (Wbni).[144] The NIS Directive was implemented in various ways in different EU Member States, e.g. regarding the scope and security requirements.[145] For this reason, the NIS Directive was repealed and replaced by the NIS 2 Directive, with the new directive containing more minimum rules and a broader scope of sectors and activities that are subject to cybersecurity obligations.[146] The goal of the NIS 2 Directive is minimum harmonisation. Therefore, it does not preclude the Netherlands from adopting other measures that ensure a higher level of cyber security than what follows from the directive.[147]

[141] Art. 1(1) NIS 2 Directive.

[142] The transposition deadline is October 17th 2024 ex art. 41 NIS 2 Directive.

[143] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) (*OJ* 2016, L194/1).

[144] Wet beveiliging netwerk- en informatiesystemen (*Stb*. 2022, 441).

[145] Consideration 4 NIS 2 Directive.

[146] Consideration 5 NIS 2 Directive.

[147] Art. 5 NIS 2 Directive.

The directive considers, i.a., Member States' central governments 'essential entities'.[148] Public administration entities in the area of "national security, public security, defence or law enforcement" are exempted.[149] Therefore, the obligations in the directive do not apply to the Ministry of Defense. The Netherlands has to ensure, via its transposition, that the other ministries, as parts of the Dutch central government, take "appropriate and proportionate technical, operational and organisational measures to manage the risks to the security of network and information systems […]".[150] The Netherlands furthermore has to ensure that corrective measures are taken in case of non-compliance.[151]

The Dutch government intends to fill in this prescribed duty of care by grounding its current information security baseline for the government (BIO), as part of transposing the directive into Dutch law.[152] The BIO is mandatory for the central government as a ministerial instruction (circulaire), which could be more firmly grounded in law. Section 3.2.1 will elaborate on the current BIO's obligations for storing government data in the cloud.

3.1.2 The European Cloud Certification Scheme

Another form of EU influence concerns the proposed European Cybersecurity Certification Scheme for Cloud Services based on the Cybersecurity Act.[153] The goal of a cybersecurity scheme under this regulation is to "increase the level of cybersecurity within the Union".[154] Providers of ICT products, services or processes, such as cloud providers, can have their products, services or processes certified under such a scheme. This is, in principle, not mandatory, but it could be made mandatory in (other) EU law or Member State law.[155] The

[148] Art. 3(1)(d) jo. Art. 2(2), point (f)(i) NIS 2 Directive.

[149] Art. 3(7) jo. 3(8) NIS 2 Directive.

[150] Art. 21(1) NIS 2 Directive. Those measures should at least include the ones mentioned in Art. 21(2)(a-j).

[151] Art. 21(4) NIS 2 Directive.

[152] 'Mapping NIS2-maatregelen', digitaleoverheid.nl; *Kamerstukken II* 2022/23, 26643, nr. 917, p. 2-3; Appendix with *Kamerstukken II* 2022/23, 26643, nr. 940, p. 30.

[153] Title III Cybersecurity Act.

[154] Art. 46(1) Cybersecurity Act.

[155] Art. 56(2) Cybersecurity Act.

security objective of a European cybersecurity certification scheme should, i.a., be to protect data against “unauthorised storage, processing, access or disclosure”.[156]

In December 2020, ENISA published the first proposal of the EUCS.[157] This proposal did not contain any requirements on where data should be stored or whether cloud service providers can be subject to the jurisdiction of third countries.[158] Multiple countries and the European Commission have since lobbied to introduce such obligations in the scheme for services where the highest assurance level is required.[159]

An elaboration on this discussion and an analysis of the underlying arguments will be provided in section 4.2.1 Relevant for this part is the fact that certification under the EUCS could be made mandatory under art. 21 of the NIS 2 Directive for essential entities or the services they use. Furthermore, governments could require such a certification as a requirement in public procurement procedures. Additionaly, including such ‘data sovereignty requirements’ for certain types of cloud services in the EUCS could itself signal that such cloud services are considered more secure.[160] Organizations themselves could then choose to require such a certification to show compliance with e.g. the duty of care in the NIS 2 Directive.

3.2 The Dutch legal and policy framework

3.2.1 Information security baseline for the government

The BIO is a common framework of information security standards based on the international standards for information security ISO 27001 and 27002. The BIO contains norms and concrete measures that must be complied with by the whole government.[161] Because the BIO only binds parts of the government, external cloud service providers are not bound by it.[162] The Information Security Regulation (VIR) and Information Security Regulation – Special

[156] Art. 51(a) Cybersecurity Act.

[157] ENISA 2020.

[158] Michels, Millard & Walden 2023, p. 53.

[159] Michels, Millard & Walden 2023, p. 53-54; Propp 2022.

[160] Michels, Millard & Walden 2023, p. 55-56.

[161] BIO, p. 1, 4-5.

[162] BIO, p. 11.

Information (VIRBI 2013) prescribe additional measures for the central government and will be discussed in section 3.2.2.

The BIO prescribes a risk-based approach where the risk management is proportional to the relevant interests and threats. For this approach, BIO distinguished three basic security levels (BBNs). Additional mandatory measures compared to the lower level are described for each BBN. In the current version of BIO, the additional measures for BBN 3 are not yet described.[163] The BBNs are determined based on the required confidentiality, integrity and availability of the information. The required level is, in turn, based on the consequences of a breach of one of these aspects for the organization. A summary is given in Table 1.

Table 1. BBN level based on the required confidentiality, integrity and availability (Source: BIO, p. 32-32)

Basic security level (BBN)	Confidentiality	Integrity	Availability
1	Low	Low	Low
2	Medium	Medium	Medium
3	High	Medium	Medium

BBN 2 is considered the starting point for government data.[164] In the case of state secrets and other cases when resistance to state actors is necessary, BBN 3 applies.[165]

Because public cloud providers are external service providers, the use of cloud services is regulated in Chapter 15 (vendor relations) of the BIO.[166] The prescribed measures in that chapter aim 'to ensure the protection of organisation's assets that are accessible to suppliers', which could involve government data.[167] The BIO does not contain specific requirements on data sovereignty or the jurisdiction under which the service provider falls. It does, however, contain the obligation to determine confidentiality, integrity and availability requirements in the contract for all BBNs.[168] For BBN 2 and higher, an explicit risk assessment should be

[163] BIO, ftn. 24.

[164] BIO, p. 9.

[165] BIO, p. 34.

[166] See also *Kamerstukken II* 2022/23, 26643, nr. 963, p. 4.

[167] BIO, p. 28.

[168] BIO 15.1.1.1.

made concerning the service provider's access to data, and mitigation measures should be determined.[169]

The BIO does not contain specific obligations on the use of cloud services, nor does it exclude the use of public cloud services. It prescribes certain mandatory procedures and elements of the contract with the cloud service provider. The BIO requires making risks explicit and determining mitigation measures, but it does not clearly determine how the risk of third-country jurisdiction applying to cloud service providers should be weighed.

3.2.2 Information security regulation (Special Information)

The VIRBI 2013, a ministerial decree, concerns the information security of special information (‘bijzondere informatie’) of the Rijksdienst.[170] The Rijksdienst is defined as all organisational units for which ministerial responsibility applies.[171]

The ministerial decree imposes a classification requirement for information whose secrecy is required because of the interest of the State, its allies or one or more ministries.[172] The classification depends on the expected negative consequences in relation to those interests.[173] Table 2 shows the different classification categories and relates them to the BIO BBNs.

[169] BIO 15.1.1.2.

[170] Art. 2(1) VIRBI 2013.

[171] Art. 1(g) VIRBI 2013.

[172] Art. 4(1) VIRBI 2013.

[173] Jansen 2021, p. 254.

Table 1. Classification and conditions of special information (Source: Art. 4(2) VIRBI 2013; BIO, p. 9)

Classification	Condition	BBN
State secret top secret (Stg.ZG)	If knowledge by unauthorised persons could cause very serious damage to any of the vital interests of the State or its allies	3
State secret secret (Stg.G)	If knowledge by unauthorised persons could cause serious damage to any of the vital interests of the State or its allies	3
State secret confidential (Stg.C)	If knowledge by unauthorised persons could cause damage to any of the vital interests of the State or its allies	3
Departmentally confidential (Dep.V.)	If knowledge by non-authorised persons could damage the interests of one or more ministries.	2 or 3, depending on whether resistance to threats from State actors or professional criminals is required

The State's vital interests include five aspects: territorial safety, physical safety, economic safety, ecological safety and social and political stability.[174] Territorial safety is defined as "the undisturbed functioning of the Netherlands as an independent state, and in particular, the territorial integrity of its territory and its international position".[175] Territorial integrity is thus seen as one element of the undisturbed functioning of the Netherlands as an independent state, which itself is one of its vital interests. The interest of one or more ministries concerns the undisturbed functioning in performing its duties and realising its goals.[176] Determining the correct classification will depend on interpreting the aforementioned interests and has an arbitrary aspect.[177]

[174] See also appendix with *Kamerstukken II* 2006/7, 30821, nr. 3.

[175] VIRBI 2013, p. 11.

[176] VIRBI 2013, p. 11.

[177] Jansen 2021, p. 254-255.

The information security measures are based on risk management.[178] The definition of information security is provided in the VIR, to which the VIRBI 2013 is a supplement.[179] It is 'the process of establishing the required reliability of information systems in terms of confidentiality, availability and integrity as well as establishing, maintaining and monitoring a coherent set of associated measures'.[180]

VIRBI 2013 Appendix 1 outlines design principles for an adequate system of security measures to safeguard special information, which should be applied more stringent based on the classification level. Those principles concern (i) protection in multiple layers, so there is no dependency on one protection measure (ii) authorisation on a need-to-know basis, (iii) systems not trusting other systems unless proven otherwise and (iv) periodic controls of the measures taken by the internal security officer or the accreditation authority.

The VIRBI 2013 does not explicitly mention data sovereignty or the use of cloud services. However, when parts of the (storage) services are outsourced, the same level of security has to be realised as applicable to internal services for all classifications.[181] At the same time, the security level should correspond to the risk.[182] Since hosting government data in a public cloud could introduce the risk of government data being disclosed to third countries, such as the US, additional security measures should be taken to sufficiently mitigate this risk. A public cloud service cannot be used if this is not possible, according to VIRBI 2013.

3.2.3 National cloud policy and risk assessment framework

In 2022, the state secretary assigned to the portfolio of digital government published the national cloud policy, adopted by the Dutch Council of Ministers,[183] in her letter to the parliament. This cloud policy was adopted by the Dutch Council of Ministers.[184] This policy presented a new mandatory policy for the central government's use of public cloud services. It replaces the 2011 policy, which aimed at using a private cloud maintained by the

[178] Art. 6(2) VIRBI 2013.

[179] Art. 2(2) VIRBI 2013.

[180] Art. 1(a) VIR.

[181] Art. 7(1) and Appendix 1(5)(D) VIRBI 2013.

[182] Appendix 1(5)(C) VIRBI 2013.

[183] National cloud policy.

[184] *Kamerstukken II* 2022/23, 26643, nr. 963, p. 16.

government.[185] At the time, the market for public cloud services was deemed immature for governments to use because those services could not meet the government's requirements regarding their responsibilities and cybersecurity.[186] The policy had a "strict requirement" that all data should be kept in the Netherlands.[187] Furthermore, the goal was to establish a private cloud for data storage and e-mail services.[188]

The private cloud was, however, never fully established because no assessment of the common needs of the different ministries was done.[189] Furthermore, in the 'Strategic ICT Agenda Rijksdienst' in 2016, public cloud services (SaaS, PaaS and IaaS) were mentioned as an option for the central government, provided that a risk assessment would be made.[190] This was done without withdrawing the old national cloud policy. The aim of the new national cloud policy is to resolve the ambiguity resulting from this.[191] The new national cloud policy regulates the use of public cloud services by the central government and follows the NIST definition of cloud computing (see section 2.2).[192] The Ministry of Defence is placed outside the policy scope. All central government organizations are mandated to create their own cloud policy and strategy within the limits of the national cloud policy.[193]

The policy takes as its starting point that public cloud services can only be used based on a 'relevant risk assessment'.[194] This risk assessment is elaborated in the Risk assessment framework, which will be further explained below. An additional regime is introduced for four government data types, summarized in Table 3.

[185] *Kamerstukken II* 2010/11*,* 26643, nr. 179.

[186] *Kamerstukken II* 2010/11, 26643, nr. 179, p. 2.

[187] *Kamerstukken II* 2010/11, 26643, nr. 179, p. 3.

[188] *Kamerstukken II* 2014/15, 33326, nr. 13, p. 32-33.

[189] National cloud policy, p. 6.

[190] Appendix with *Kamerstukken II* 2016/17, 31490, nr. 221, p. 19.

[191] National cloud policy, p. 8.

[192] National cloud policy, p. 7.

[193] National cloud policy, p. 2.

[194] National cloud policy, p. 2.

Table 3. Public cloud policy regarding sensitive categories of data. (Source: National cloud policy, p. 4-5)

Type of government data	Can it be stored in the public cloud?
State secrets[195]	No
Personal data[196]	Yes, provided that storage and processing takes place (i) in the European Economic Area or (ii) in a country with an adequacy decision (Art. 45(3) GDPR) or (iii) when the transfer is subject to appropriate safeguards (Art. 46 GDPR)
Special categories of personal data[197]	No, unless storage and processing takes place (i) in the European Economic Area or (ii) in a country with an adequacy decision (Art. 45(3) GDPR) or (iii) when the transfer is subject to appropriate safeguards (Art. 46 GDPR) and an additional explanation is provided
'Basisregistraties'[198]	No, unless an explanation is provided

Public cloud services cannot be used for any state-secret information, which is information that could damage any of the vital interests of the State (see section 3.2.2).[199] This is based on a non-public memo of the AIVD from January 2021, which advised excluding the use of cloud services for state secrets and determining the use of a public service for departmentally confidential information on a case-by-case basis.[200] This is a change in position compared to 2019 when the intelligence agency also excluded the use of public cloud services for departmentally confidential information. Back then, the AIVD had insufficient assurance that public cloud services could comply with the VIRBI 2013 and BIO requirements for any classified information.[201] During a verbal explanation of the memo, the AIVD stated that the

[195] Art. 4(2)(a-c) VIRBI 2013.

[196] Art. 4(1) GDPR.

[197] Art. 9(1) GDPR.

[198] A centralised government-wide data infrastructure with vital and authentic data on citizens, companies and other organisations, see 'Stelsel van basisregistraties', digitaleoverheid.nl.

[199] National cloud policy, p. 2.

[200] National cloud policy, p. 11-12. See also *Kamerstukken II* 2022/23, 26643, nr. 963, p. 16.

[201] NORA 2022.

shift in position resulted from the observation that some public cloud services can be more secure than self-hosted solutions.[202] Furthermore, it wanted to accommodate the wish of government organizations to use the public cloud.

When personal data[203] is concerned, a pre-scan data protection impact assessment (pre-scan DPIA) is mandatory, and depending on the outcome, a formal data protection impact assessment (DPIA) should be carried out.[204] Personal data can, in principle, be stored in the public cloud, provided Chapter V of the GDPR is complied with. The policy on storing special categories of personal data is worded in reverse, which could have an implication on the mandatory risk assessment. Basisregistraties cannot be stored in the public cloud, but exceptions are possible. The policy gives no indication of what would justify such an exception.

A risk assessment on using a public cloud service should consider at least the type of cloud service (SaaS, PaaS or IaaS), the sensitivity of the type of data and the geographical region of the data storage.[205] Furthermore, the 'residual risks' identified by the AIVD, should be considered.[206] One of these identified risks is when the country of the cloud service provider has gained access to the data via extra-territorial judicial possibilities.[207] In addition, the framework developed around purchasing a new communication system for emergency services in 2019, the C2000-criteria, should be considered.[208] These criteria mainly exclude products and services from states with active offensive intelligence programmes against the Netherlands.[209] However, one of the criteria mentions the situation when a service provider is forced to cooperate with a third country based on its legislation, especially concerning state surveillance. A service provider should be excluded when possible if national security risks cannot sufficiently be mitigated.[210] Lastly, the national cloud policy prescribes that public

[202] Personal correspondence with the memo's author (AIVD) in a call on 21 June 2024.

[203] Within the meaning of Art. 4(1) GDPR.

[204] Art. 8 Risk assessment framework; National cloud policy, p. 1, 4.

[205] Art. 4(3)(a) Risk assessment framework.

[206] Art. 4(3)(b) jo. Appendix 2 Risk assessment framework.

[207] Appendix 1 Risk assessment framework.

[208] Art. 4(3)(b) jo. 6 jo. Appendix 1 Risk assessment framework.

[209] *Kamerstukken II* 2018/19, 25124, nr. 96.

[210] Art. 6(3) Risk assessment framework.

values should be considered when selecting a cloud service provider, “like open source, human rights and sustainability”.[211]

3.3 Subconclusion

This chapter described the legal and policy framework for storing Dutch government data in the public cloud. The NIS 2 Directive requires the Netherlands to introduce a duty of care for central government organizations. The Dutch government plans to do so via the already mandatory BIO. This cybersecurity regulation prescribes data and IT systems measures on three levels, depending on the required confidentiality, integrity and availability (BBNs). Because public cloud service providers are external and the BIO binds only government organizations, only chapter 15 on vendor relations is relevant. Risks should be made explicit based on a risk assessment, and mitigation measures should be determined. The VIRBI 2013 prescribed cybersecurity measures for classified information on four levels. The AIVD held that various risks for state secrets could not sufficiently be mitigated in the public cloud. Therefore, public cloud services are explicitly excluded for state secrets in the national cloud policy. It is allowed for departmentally confidential information and non-classified information, but on a case-by-case basis following a risk assessment. Additional measures could apply for personal data, such as performing a DPIA.

[211] Art. 5(3) Risk assessment framework.

4. Government data sovereignty and the Dutch approach

This chapter will analyse the Dutch legal and policy framework, as described in section 3.2, based on the concept of government data sovereignty as described in Chapter 2. It is defined as "Government's exclusive authority […] over all virtual public assets, which are not in the public domain, irrespective of whether they are stored on their own or third parties' facilities and premises".[212] The critique in the literature on the national cloud policy will also be discussed. The discussion on the EUCS will be highlighted to further contextualise the Dutch rationales behind the legal and policy framework on the use of public cloud services.

4.1 Government data sovereignty in the Dutch legal and policy framework

The concept of government data sovereignty itself is not mentioned in the identified legal and policy framework. However, the framework for storing government data in the public cloud can be said to take a relative approach to protecting government data sovereignty. Different cybersecurity measures apply depending on the sensitivity and type of data and can protect government data from the risk of being subject to the jurisdiction of a third country. Overall, the approach is risk-based.

The VIRBI 2013 prescribes requirements for classified government data on four levels and takes a risk-based approach.[213] The AIVD advised that state secret government data risks cannot be sufficiently mitigated. Following the advice, the Dutch government excludes the use of public cloud services for these most sensitive types of government data in its national cloud policy.[214] This exclusion is, therefore, not based on a categorical decision to exclude public cloud service subject to the jurisdiction of a third country and protect government data sovereignty. It is based on a general risk assessment.

A risk assessment should be made before using a public cloud service for government data classified as departmentally confidential and other types of government data. The prescribed risk assessment contains a few elements relevant to protecting government data sovereignty. First of all, the type of cloud service (SaaS, PaaS, IaaS), the sensitivity of the

[212] Irion 2012, p. 41.

[213] Art. 6(2) VIRBI 2013.

[214] Art. 1(f) Risk assessment framework.

type of data and the geographical region of storage should be considered.[215] Next to that, the risk assessment should consider the C2000 criteria (see section 3.2.3) on the threats of state actors and the risks to the use of cloud services identified by the AIVD.[216] Although the C2000 criteria mention the risk of extra-territorial jurisdiction,[217] it is in relation to the national cloud policy primarily cited to highlight the risk of countries with active offensive intelligence programmes against the Netherlands.[218]

The national cloud policy does mention the risk of extra-territorial legislation such as the CLOUD Act and FISA to sensitive government data. It argues that this risk is sufficiently mitigated by excluding state secrets from being stored in the public cloud and by performing a risk assessment as described above.[219] Lastly, if government data sovereignty is considered a public value, it must be considered when selecting the cloud service provider.[220] It is, however, not mentioned as one of the examples in the non-exhaustive list. Nor is it clear how public values should be weighed in the risk assessment.[221]

4.1.1 A risk-based approach

Even though the national cloud policy and the rest of the framework prescribe a risk assessment for storing government data in the public cloud, it is not sufficiently clear which level of risk is acceptable. The risk assessment framework does prescribe to include data sovereignty-related risks, but it is unclear to what extent this should be considered. Full data sovereignty is effectively guaranteed for state secrets since the public cloud cannot be used for this type of government data. This is, however, the result of a general risk assessment of the AIVD and not the result of prescribed data sovereignty requirements.

The AIVD-commissioned report criticizes the national cloud policy on the point that the risk assessment and implementation have to be done by IT departments of government organizations. It is argued that technical advantages will be better considered than the country

[215] Art. 4(3)(a) Risk assessment framework.

[216] Art. 4(3)(b) jo. Appendix 1 jo. Appendix 2 Risk assessment framework.

[217] Appendix 1(1) Risk assessment framework.

[218] See e.g. National cloud policy, p. 3 and *Kamerstukken II* 2022/23, 26643, nr. 963, p. 15.

[219] National cloud policy, p. 11-12.

[220] Art. 5(3) Risk assessment framework.

[221] See also *Kamerstukken II* 2022/23, 26643, nr. 976.

of origin of the cloud service provider and the related risks to data sovereignty.[222] This could be seen as a result of the risk assessment framework being unclear on to what extent data sovereignty should be considered and only fully safeguarding it for state secrets. Krikke argues that the prescribed risk assessment focuses too much on personal data at the cost of more sensitive government data not being state secrets.[223] To better protect data sovereignty, the risk assessment could, therefore, be better specified for different types of sensitive government data. Although data sovereignty is safeguarded for state secrets, it is unclear, based on the current risk assessment framework, to what extent other sensitive government data is being protected from the risk of the jurisdiction of a third country applying, either via territoriality or the could provider's nexus with a third country, which could have consequences for the confidentiality, availability or integrity of government data.

It could be that government organizations further specify this in their own cloud policies and strategies, which they are obliged to make within the limits of the national cloud policy.[224] Given the importance of government data sovereignty, however, the national cloud policy could have prescribed more requirements regarding data sovereignty or to what extent this should be considered in the risk assessment. Even though individual risk assessments could consider the risk to data sovereignty low for a specific set of government data within a government organization, the collective detriment to government data sovereignty as a whole could become too high.

Moerel & Timmers identify the risk management approach as one of the possible approaches to achieving digital sovereignty, of which data sovereignty can be seen as a part.[225] This approach prescribes risk-based cybersecurity regulations. The identified framework clearly follows this approach. Another approach could be to limit third parties, such as cloud service providers, to certain exceptions.[226] An example of this in the context of data sovereignty would be to require cloud service providers, for certain types of data, to not be subject to the jurisdiction of third countries. This would safeguard data sovereignty, regardless of a risk assessment.

[222] Gomes & Okano-Heijmans 2024, p. 11.

[223] Krikke 2022, p. 188.

[224] Art. 1(b) Risk assessment framework.

[225] Moerel & Timmers 2021, p. 19.

[226] Moerel & Timmers 2021, p. 19.

France is a prominent example of following this approach. The country has a national cloud certification scheme (SecNumCloud), which requires cloud service providers to be immune from non-EU law to be certified at the highest level.[227] Next to this, the SecNumCloud certification is mandatory when French government organizations procure public cloud services to store sensitive data.[228] France, together with Germany, Italy and Spain, also lobbied for introducing such sovereignty requirements in the European certification scheme EUCS (see section 3.1.2). The strongest opponent of this suggestion has been the Netherlands.[229] Therefore, the next section will discuss the arguments exchanged in this debate on data sovereignty requirements to discuss the different approaches. This will also allow for further evaluation of the Dutch framework for storing government data using public cloud services.

4.2 The European Cloud Certification Scheme

4.2.1 The course of the discussion

The first EUCS proposal by ENISA did not contain any requirements on whether cloud service providers can be subject to the jurisdiction of third countries.[230] In the discussion following the proposal, the European Commission and France, Germany,[231] Italy and Spain proposed to include sovereignty requirements at the highest certification level to "adequately prevent and limit possible interference from states outside of the EU with the operation of certified cloud services".[232] The Netherlands, Sweden, and Ireland responded to the subsequent draft with a non-paper, arguing that the proposed requirements could impact the ability of cloud service providers to develop their services and compete on the global market.[233] It was also argued that adding such requirements would be protectionist and "have nothing to do with cybersecurity concerns".[234] The Netherlands gathered a coalition of countries to oppose the sovereignty requirements that were part of subsequent drafts. In late

[227] Rone 2024, p. 11.

[228] Propp 2022.

[229] Rone 2024, p. 10; Bertuzzi 2023b.

[230] ENISA 2020.

[231] Germany later changed its position after resistance from German businesses, see Rone 2024, p. 14-15.

[232] Kabelka 2022.

[233] Kabelka 2022.

[234] Kabelka 2022; See also Rone 2024, p. 12-13, Bertuzzi 2022 and Bertuzzi 2023a.

2023, the Dutch state secretary assigned to the portfolio of digital government stated: "We see the risk that the sovereignty requirements included in the scheme will create unfair competition between the EU member states and might also result in a market access barrier, which could negatively impact our strategic partnerships with countries like the US and Japan."[235]

The EUCS is still under negotiation. The data sovereignty criteria were deleted in the latest version (March 2024).[236] The opposing coalition of mostly smaller countries argued that the data sovereignty criteria would prevent them from being able to use "top-notch cloud services".[237] The latest version, however, allowed individual countries to set data sovereignty standards on top of the EUCS scheme. Large EU-based cloud service providers, such as OVHcloud, Deutsche Telekom and Capgemini, responded to the latest draft with a joint statement. They called for reintroducing data sovereignty requirements, i.a., to address the security risk of unlawful data access in the scheme.[238]

4.2.2 Government data sovereignty requirements

As discussed in Chapter 2, government data sovereignty related risks can be seen as security risks, since they relate to detriment to the confidentiality, integrity and/or availability of government data. From that perspective, including a requirement to not be subject to the jurisdiction of a third country is consistent with the goal of ensuring a high level of security.

The main argument against data sovereignty requirements (for the most sensitive types of data) is thus the argument against protectionism. Such an argument does, however, not address the real concern of government data being subject to the jurisdiction of third countries.[239] It argues that adding data sovereignty related requirements is an interventionistic policy that promotes domestic service providers at the cost of foreign competitors. This would hinder competition and innovation. The Netherlands opposes the data sovereignty requirements in the EUCS for this reason.[240] This "liberal, business-led approach"[241] is also

[235] Bertuzzi 2023b.

[236] ENISA 2024.

[237] Gkritsi 2024.

[238] A1 et al. 2024, p. 1.

[239] See also Chander & Sun 2024, p. 24-26; Kristakis 2024, p. 387; Kuner 2015, p. 2097-2098.

[240] Rone 2024, p. 12-13.

[241] Rone 2024, p. 12.

visible in the national cloud policy, where no public cloud services providers are excluded based on data sovereignty concerns for all unclassified information and information classified as departmentally confidential.

Data sovereignty requirements could, in turn, positively impact the growth of the EU cloud services in the cloud market, being able to comply with the requirement of not falling under the jurisdiction of third countries.[242] European cloud providers also argue that such requirements would create a level playing field because of the current dominance of US hyper scalers.[243]

4.3 Subconclusion

Government data sovereignty should be a legitimate concern for nation states. Currently, the Netherlands takes a risk management approach, mandating risk assessments before public cloud service providers are used. Only classified state secrets are explicitly excluded from using public cloud services, following the general risk assessment of the AIVD. The current national cloud policy and risk assessment framework do not explicitly mention data sovereignty.

The national cloud policy focuses mainly on classified information and personal data while leaving the risks to other types of sensitive government data underexposed, although they are included as elements of the risk assessment framework. To protect Dutch government data sovereignty more adequately, the Netherlands could adopt data sovereignty requirements for more types of data than only state secrets. Furthermore, the risk assessment framework and the national cloud policy could define more clearly how data sovereignty should be weighed in the risk assessment compared to advantages such as usability. This could be done by further distinguishing between different types of sensitivity of government data, compared to the current approach. The C2000 criteria are mentioned in the risk assessment framework, but mainly in the context of state actors with active offensive intelligence programmes against the Netherlands. This leaves the risk to government data sovereignty as a result of public cloud service providers falling under the jurisdiction of a third country unaddressed. In addition, government data sovereignty could be more explicitly

[242] For an extensive discussion on the relationship between data sovereignty and promoting the European cloud ecosystem, see e.g. Blancato 2023.

[243] Pollet 2022.

considered a public value, so it must be considered when central government organizations select the public cloud service provider.[244] This would imply a deviation from the current market-oriented approach, which is also apparent in the discussion on the EUCS.

[244] Art. 5(3) Risk assessment framework.

5. Conclusion

The Dutch government's approach to using public cloud services proved highly controversial. Public cloud services such as AWS offer benefits in terms of scalability and cost-efficiency, but is government data adequately protected from the jurisdiction of third countries? The central question of the research was: *How does the Dutch legal and policy framework on hosting government data in a public cloud protect Dutch government data sovereignty, and why does this matter?* Government data sovereignty was defined as governments having exclusive authority over their data. It was identified as a relative concept, meaning that different standards should apply depending on the sensitivity of the data. Relating the concept to cybersecurity, government data sovereignty describes the exclusive authority over the confidentiality, integrity and availability of government data.

Public cloud services have advantages for governments, such as scalability and cost efficiency. The Dutch government mainly uses cloud services from US service providers. The security could be higher depending on the specific service offered, but using cloud service providers under concurrent jurisdiction, i.e. US jurisdiction, poses an additional security threat compared to a self-hosted solution. The US claims, via the principle of personal jurisdiction, jurisdiction over US service providers, their subsidiaries and any company with sufficient contacts with the US, regardless of where it's based. This allows the US to compel cloud service providers via legislation such as the CLOUD Act (law enforcement) and FISA section 702 (intelligence agencies) to hand over customer data, which could be government data. This matters because it would impact the confidentiality of sensitive government data and the state's integrity.

Additional measures like encryption and adequate key management could lower the risk. This is, however, not always possible or viable for all types of cloud services, such as SaaS and is dependent on the implementation of the cloud service provider. Furthermore, the risk to data availability cannot be fully mitigated because the US could compel cloud service providers to change the service in the future based on their claimed jurisdiction. A contract between the Dutch government and the cloud service provider has no external effect and cannot fully prevent these government data sovereignty issues.

The Dutch legal and policy framework for hosting government data in a public cloud does not explicitly mention data sovereignty. It takes a risk-based approach to the use of cloud services. Based on the advice of the AIVD, information classified as state secrets cannot be stored in a public cloud. This effectively guarantees data sovereignty for state secrets. A risk assessment should be made for all other types of government data, including information classified as departmentally confidential. Additional measures apply to personal data. The risk assessment framework accompanying the national cloud policy includes some criteria relevant to data sovereignty, such as the type of cloud service, the sensitivity of the data and the possibility of taking mitigating measures. This potentially offers some protection. However, it is unclear how the risk to data sovereignty should be weighed in this risk assessment compared to, for example, the alleged benefits of self-hosted solutions. This is arguably a political question, depending on the willingness to spend resources on security for a self-hosted solution or an alternative that would better protect government data sovereignty but is more expensive and perhaps has fewer features. A way to better protect government data sovereignty in the Dutch legal and policy framework could be to introduce data sovereignty requirements for additional sensitive types of data, which would require a cloud service provider not to fall under the jurisdiction of a third or non-EU country. This would require the Netherlands to deviate from the current market-oriented risk-based approach that is also apparent in its stance in the European Cloud Certification Scheme discussion.

Future research could analyse the protection of government data sovereignty from a more empirical (legal) perspective, e.g. by analysing public procurement procedures. It could also research the impact of other recent EU legislation, such as the Data Act,[245] which was out of scope for this thesis. Lastly, mainly using foreign cloud service providers has effects extending beyond compromising government data sovereignty, which could merit future research.[246] It, for example, impacts the government's in-house knowledge of providing self-hosted solutions. This results from IT personnel being required to know how to migrate to and use public cloud services instead of maintaining self-hosted solutions. The impact of the current framework is, therefore, not only on government data sovereignty but also on autonomy.

[245] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (*OJ* 2023, L 2023/2854)

[246] See e.g. Hubert 2024.

6. Bibliography

Literature

Abraha 2020

H.H. Abraha, ‘Regulating law enforcement access to electronic evidence across borders: the United States approach’, *Information & Communications Technology Law* (29) 2020, afl. 3, p. 324-353.

Ali, Khan & Vasilakos 2015

M. Ali, S.U. Khan & A.V. Vasilakos, ‘Security in cloud computing: Opportunities and challenges’, *Information Sciences* (305) 2015, p. 357-383.

Alouffi et al. 2021

B. Alouffi et al., ‘A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies’, *IEEE Access* (9) 2021, p. 57792-57807.

Blancato 2023

F.A. Blancato, ‘The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem’, *Policy & Internet* (16) 2024, afl. 1, p. 12-32.

Chander & Sun 2024

A. Chander & H. Sun, ‘Introduction: sovereignty 2.0’, in: A. Chander & H. Sun (eds.), *Data Sovereignty: from the digital silk road to the return of the state*, Oxford: Oxford University Press 2024, p. 1-31.

Christakis 2024

T. Christakis, ‘European Digital Sovereignty, Data Protection, and the Push toward Data Localization’, in: A. Chander & H. Sun (eds.), *Data Sovereignty: from the digital silk road to the return of the state*, Oxford: Oxford University Press 2024, p. 371-389.

Couture & Toupin 2019

S. Couture & S. Toupin, ‘What does the notion of ‘sovereignty’ mean when referring to the digital?’, *New Media & Society* (21) 2019, afl. 10, p. 2305-2322.

Van Dijck, Snel & Van Golen 2018

G. van Dijck, M. Snel & T. van Golen, *Methoden van rechtswetenschappelijk onderzoek*, Den Haag: Boom juridisch 2018.

Hildén 2021

J. Hilden, 'Mitigating the risk of US surveillance for public sector services in the cloud', *Policy & Internet* (10), afl. 3, p. 1-23.

Gürses & Van Hoboken 2018

S. Gürses & J. van Hoboken, 'Privacy after the Agile Turn', in: E. Selinger, J. Polonetsky & O. Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge: Cambridge University Press 2018, p. 579-601.

Gomes & Okano-Heijmans 2024

A. Gomes & M. Okano-Heijmans, *Too Late to Act? Europe's Quest for Cloud Sovereignty* (Clingendael Institute Policy Brief), 2024, clingendael.org.

Hon, Millard & Singh 2022a

W.K. Hon, C. Millard & J. Singh, 'Cloud Computing Demystified (Part 1): Technical and commercial fundamentals' (author-edited version), in: C. Millard (ed.), *Cloud Computing Law*, Oxford: Oxford University Press 2022, https://dx.doi.org/10.2139/ssrn.4030064.

Hon, Millard & Singh 2022b

W.K. Hon, C. Millard & J. Singh, 'Cloud Computing Demystified (Part 2): Control, Security, and Risks in the Cloud' (author-edited version), in: C. Millard (ed.), *Cloud Computing Law*, Oxford: Oxford University Press 2022, https://dx.doi.org/10.2139/ssrn.4030114.

Hummel et al. 2021

P. Hummel et al., 'Data sovereignty: A review', *Big Data & Society* (8) 2021, afl. 1, p. 1-17.

Irion 2012

K. Irion, 'Government Cloud Computing and National Data Sovereignty', *Policy & Internet* (4) 2012, afl. 3/4, p. 40-71.

Jansen 2021

R.H.T. Jansen, 'Regeling vertrouwelijke stukken van de Tweede Kamer', *Tijdschrift voor Constitutioneel Recht* 2021/21, afl. 4, p. 251-265.

Kestemont 2015

L. Kestemont, 'A meta-methodological study of Dutch and Belgian PhDs in social security law: devising a typology of research objectives as a supporting tool', *European Journal of Social Security* (17) 2015, afl. 3, p. 361-384.

Krikke 2022

J. Krikke, ‘Opinie - Kamerbriek Rijksbreed cloudbeleid 2022’, *Tijdschrift voor Internetrecht* 2022, afl. 5, p. 187-188.

Kuner 2015

C. Kuner, ‘Data Nationalism and Its Discontents’, *Emory Law Journal Online* (64) 2015, p. 2089-2098.

Michels, Millard & Walden 2023

J.D. Michels, C. Millard & I. Walden, ‘On Cloud Sovereignty: Should European Policy Favour European Clouds?’, *Queen Mary Law Research Paper Series* 412/2023, p. 1-68.

Michels & Millard 2022

J.D. Michels & C. Millard, ‘The new things: property rights in digital files?’, *The Cambridge Law Journal* (81) 2022, afl. 2, p. 323-355.

Mignon 2020

E. Mignon, ‘The CLOUD Act: Unveiling European Powerlessness’, *RED* (1) 2020, afl. 1, p. 108-116.

Moerel & Timmers 2021

E.M.L. Moerel & P. Timmers, *Reflections on Digital Sovereignty*, EU Cyber Direct 2021.

Propp 2022

K. Propp, ‘European Cybersecurity Regulation Takes a Sovereign Turn’, europeanlawblog.eu, 12 September 2022.

Rone 2024

J. Rone, ‘”The Sovereign cloud” in Europe: diverging nation state preferences and distputed institutional competences in the context of limited technological capabilities’, *Journal of European Public Policy* 2024, special issue *Digital Sovereignty - Rhetoric and Reality*, p. 1-27, DOI:10.1080/13501763.2024.2348618.

Snel & Vranken 2019

M. Snel & J. Vranken, ‘Het gefinancierde rechtswetenschappelijke onderzoek onder de loep’, Ars Aequi 2019, p. 712-719.

Svantesson et al. 2023

Svantesson et al., ‘On Sovereignty’, *Masaryk University Journal of Law and Technology* (17) 2023, afl. 1, p. 33-85.

Taekema 2018

S. Taekema, ‘Theoretical and Normative Frameworks for Legal Research: Putting Theory Into Practice’, *Law and Method* 2018, p. 1-17.

Tjong Tjin Tai & Verbruggen 2022

T.F.E. Tjong Tjin Tai & P.W.J. Verbruggen, ‘Onderzoeksmethoden in de rechtswetenschap’, *NJB* 2022/2, p. 4-12.

Tweneboa-Koduah, Endicott-Popovsky & Tsetse 2014

S. Tweneboah-Koduah, B. Endicott-Popovsky & A. Tsetse, ‘Barriers to government cloud adoption’, *International Journal of Managing Information Technology* (6) 2014, afl. 3, p. 1-16.

Walden 2021

I. Walden, ‘Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent’, in: C. Millard (ed.), *Cloud Computing Law,* Oxfords: Oxford University Press 2021.

Weij 2024

M. Weij, ‘Cloudwatervrees’, *Tijdschrift voor Internetrecht* 2024, afl. 2, p. 76-78.

Wohlin 2014

C. Wohlin, ‘Guidelines for snowballing in systematic literature studies and a replication in software engineering’, *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering* 2014, afl. 38, p. 1-10.

Laws and regulations

European Union

Cybersecurity Act

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (*OJ* 2019, L 151/15).

Data Act

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (*OJ* 2023, L 2023/2854)

GDPR

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation [GDPR]) (*OJ* 2016, L 119/1).

NIS 2 Directive

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (*OJ* 2022, L 333).

NIS Directive

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) (*OJ* 2016, L194/1).

The Netherlands

Archiefwet

Archiefwet 1995 (*Stb.* 1995, 276).

BIO

Circulaire van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van 11 februari 2020 inzake het toepassen van de Baseline Informatiebeveiliging Overheid [BIO] in het digitale verkeer met het Rijk (*Stcrt.* 2020, 7857).

National cloud policy

Letter from the state secretary of the interior and kingdom relations of 29 August 2022 (*Kamerstukken II* 2021/22, 26643, nr. 904).

Risk assessment framework

Letter from the state secretary of the interior and kingdom relations of 24 January 2023 (Appendix with *Kamerstukken II* 2022/23, 26643, nr. 963).

VIRBI 2013

Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (*Stcrt.* 2013, 154970).

VIR

Besluit voorschrift informatiebeveiliging rijksdienst 2007 (*Stcrt.* 2007, 122).

Wbni

Wet beveiliging netwerk- en informatiesystemen (*Stb.* 2022, 441).

United States

FISA section 702

Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 et seq.

CLOUD Act

Clarifying Lawful Overseas Use of Data Act 2018, H.R. 4943.

Policy documents

ACM 2022

Autoriteit Consument en Markt (ACM), *Marktstudie Clouddiensten*, Den Haag: Autoriteit Consument en Markt 2022.

Article 29 Working Party 2017

Article 29 Working Party, *Data protection and privacy aspects of cross-border access to electronic evidence* (statement), 2017.

Bigo et. al 2012

Bigo et. al, *Fighting cyber crime and protecting privacy in the cloud* (PE 462.509 study for the directorate general for internal policies), 2012, europarl.europa.eu.

Breton 2022

T. Breton, ‘Europe: The Keys to Sovereignty’, ec.europa.eu/commission/presscorner, 11 September 2020.

Cyber Safety Review Board 2024

Cyber Safety Review Board, *Review of the Summer 2023 Microsoft Exchange Online Intrusion*, 2024, cisa.gov.

ENISA 2020

European Union Agency for Cybersecurity, *EUCS, a candidate cybersecurity certification scheme for cloud services*, 2020, enisa.europa.eu.

ENISA 2024

European Union Agency for Cybersecurity, *EUCS, a candidate cybersecurity certification scheme for cloud service,* 2024, https://subscriber.politicopro.com/f/?id=0000018e-a40b-d3a4-a7be-bd5f1b8b0000.

European Commission 2020

European Commission, *A European strategy for data* (COM (2020) 66 final), 2020.

European Commission 2022

European Commission, *Digital Economy and Society Index (DESI) 2022: The Netherlands*, 2022, digital-strategy.ec.europa.eu.

Greenberg Traurig 2022a

Greenberg Traurig, *Application of the CLOUD Act to EU Entities*, 2022, nscs.nl/documenten.

Greenberg Traurig 2022b

Greenberg Traurig, *Number of CLOUD Act requests*, 2022, ncsc.nl/documenten.

ICTU 2024

ICTU, *Monitor Open Standaarden 2023*, 2024, forumstandaardisatie.nl.

NIST 2018

National Institute of Standards and Technology (NIST), *Evaluation of Cloud Computing Services Based on NIST SP 800-145* (Special Publication 500-322), 2018, https://doi.org/10.6028/NIST.SP.500-322.

NIST 2011

National Institute of Standards and Technology (NIST), *The NIST Definition of Cloud computing* (Special Publication 800-145), 2011, https://doi.org/10.6028/NIST.SP.800-145.

NORA 2022

NORA, *BIO Thema Clouddiensten – Samenvatting AIVD-standpunt en beleidsverkenning BZK*, 2022, noraonline.nl.

PIAB & IOB 2023

President's Intelligence Advisory Board and Intelligence Oversight Board, *Review of FISA Section 702 and recommendations for reauthorization*, 2023, whitehouse.gov.

Parliamentary documents

Appendix with *Kamerstukken II* 2006/7, 30821, nr. 3.

Kamerstukken II 2010/11, 26643, nr. 179

Kamerstukken II 2014/15, 33326, nr. 13, p. 32-33.

Appendix with *Kamerstukken II* 2016/17, 31490, nr. 221

Kamerstukken II 2018/19, 25124, nr. 96.

Kamerstukken II 2018/19, 31066, nr. 486

Kamerstukken II 2018/19, 33694 26643, nr. 47

Kamerstukken II 2022/23, 26643, nr. 917

Appendix with *Kamerstukken II* 2022/23, 26643, nr. 940,

Kamerstukken II 2022/23, 26643, nr. 963

Kamerstukken II 2022/23, 26643, nr. 975

Kamerstukken II 2022/23, 26643, nr. 976.

Appendix with *Kamerstukken II* 2023/24, 36259, nr. 21

News articles and other online sources

A1 et al. 2024

A1 et al., 'EUCS: Ensuring full transparency and protection for European cloud users' most sensitive data is critical', https://www.linkedin.com/posts/michel-paulin-5a4042155_eucs-activity-7184081853383856128-JlHU/, 10 April 2024.

Amazon 2023

Amazon, ‘AWS Digital Sovereignty Pledge: Announcing a new, independent sovereign cloud in Europe’, aboutamazon.eu, 8 November 2023.

Bertuzzi 2022

L. Bertuzzi, ‘Germany calls for political discussion on EU’s cloud certification scheme’, euractive.com, 21 September 2022.

Bertuzzi 2023a

L. Bertuzzi, ‘EU cloud scheme slightly tones down sovereignty requirements’, euractive.com, 27 November 2023.

Bertuzzi 2023b

L. Bertuzzi, ‘Netherlands gathers opposition front to EU cloud certification scheme’, euractive.com, 7 December 2023.

Demirel, Koens & Vennekens 2023

B. Demirel, L. Koens & A. Vennekens, ‘De digitale overheid in kaart?’, rathenau.nl, 6 April 2023.

Dudely & Burke 2024

R. Dudley & D. Burke, ‘Microsoft Chose Profit Over Security and Left U.S. Government Vulnerable to Russian Hack, Whistleblower Says’, propublica.org, 13 June 2024.

Gkritsi 2024

E. Gritsi, ‘France questions latest EU cloud certification scheme’, euractiv.com, 22 April 2024.

Google 2022

Google, ‘Advancing digital sovereignty on Europe’s terms’, cloud.google.com/blog, 11 October 2022.

Hartholt 2022

S. Hartholt, ‘Waarom toestaan van commerciële clouds bij de overheid géén goed idee is’, agconnect.nl, 9 September 2022.

Hubert 2024

B. Hubert, ‘De hele overheid naar de cloud? Dat is een politiek besluit’, berthub.eu, 31 May 2024.

Hugo 2024

H. Hugo, ‘AWS krijgt nieuwe ceo en wil 7,8 miljard euro investeren in Europese cloud’, tweakers.net, 15 May 2024.

Kabelka 2022

L. Kabelka, ‘Sovereignty requirements remain in cloud certification scheme despite backlash’, euractiv.com, 21 June 2022.

Microsoft 2023

Microsoft, ‘Law Enforcement Requests Report’, microsoft.com, 2023.

Microsoft 2022

Microsoft, ‘Microsoft Cloud for Sovereignty: The most flexible and comprehensive solution for digital sovereignty, blogs.microsoft.com, 19 July 2022.

NSCS 2022

NSCS, ‘De werking van de CLOUD-Act bij dataopslag in Europa, nscs.nl/actueel/weblog, 16 August 2022.

Pollet 2022

M. Pollet, ‘European cloud providers call “not to give in to the pressure” over sovereignty requirements’, euractiv.com, 12 July 2022.

Rensen 2024

F. Rensen, ‘Rijksoverheid verhuist essentiële ict stilletjes naar buitenlandse clouddiensten, tot schrik van Kamerleden en experts’, *de Volkskrant* 4 June 2024.

The Guardian 2015.

The Guardian, ‘NSA Tapped German Chancellery for decades, WikiLeaks claims’, 9 Julu 2015.

Van Dijck & Jacobs 2022

J. van Dijck & B. Jacobs, ‘Onze overheid moet haar kostbare data niet klakkeloos uitleven aan Google en Amazon’, *de Volkskrant* 21 September 2022.