FACULTY OF LAW

LUND UNIVERSITY

Ella Virtanen

Cross-Border Data Transfers for AI Development Post-Schrems II: Balancing GDPR and AI Act Requirements

JAEM01 Master Thesis

European Business Law

15 higher education credits

Supervisor: Ana Nordberg

Term of graduation: Spring 2025

ABBREVIATIONS

The Artificial Intelligence Act - AIA
Artificial Intelligence - AI
Binding corporate rules - BCR
The Charter of Fundamental Rights of the European Union - The Charter
The Court of Justice of the European Union - CJEU
Commission Implementing Decision 2023/1795 - Adequacy Decision
Commission Nationale Informatique & Libertés - CNIL
Cybersecurity Certification Regime for Cloud Services - EUCS
Regulation (EU) 2023/2854 - Data Act
Data protection authority - DPA
The EU-US Data Privacy Framework - DPF
Data protection impact assessment - DPIA
European Free Trade Association - EFTA
The European Data Protection Board - EDPB
European Economic Area - EEA
Executive Order - EO
The European Union - EU
The European Union Agency for Cybersecurity - ENISA
Microsoft EU Data Boundary - EUDB
Foreign Intelligence Surveillance Act - FISA
The Fundamental Rights Impact Assessment - FRIA
The General Data Protection Regulation - GDPR
Standard contractual clause - SCC
Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. C-311/18. - Schrems II
Transfer impact assessment - TIA
The United States - US

TABLE OF CONTENTS

ABSTRACT

Artificial intelligence (AI) development thrives on global datasets, yet every outbound transfer of EU personal data must now satisfy two demanding regimes; the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AIA). The GDPR lets exporters rely on Adequacy Decisions, standard contractual clauses, or other Article 44-49 tools only if they can guarantee an "essentially equivalent" level of protection outside the EEA. The AIA then layers risk-based obligations, technical documentation, automated logging, bias testing, and meaningful human oversight onto high-risk AI systems, and these obligations follow the system wherever its servers or operators sit, be it outside the EEA.

The thesis investigates how, after the European Court of Justice's *Schrems II* judgment invalidated the EU-US Privacy Shield and intensified scrutiny of data exports, EU-based providers can still train, fine-tune and operate high-risk AI systems on global datasets without breaching either regime.

The analysis traces a recurring "safety chain". It begins with a GDPR data protection impact assessment (DPIA) that justifies any export of personal data; moves to a transfer impact assessment (TIA) that benchmarks third country surveillance powers against EU standards and adds encryption, pseudonymisation or other supplementary measures where gaps appear; and culminates in the AIA's fundamental rights impact assessment (FRIA), which merges those findings into AI-specific obligations such as bias testing, tamper-proof logging and human oversight.

Because the AIA's obligations travel with the system, documentation, logs and encryption keys must remain demonstrably under EU-level control even when the servers are located outside the EEA, ensuring that geography never dilutes EU Charter rights. A case study of Microsoft's EU Data Boundary shows how regional cloud strategies can reduce, but not eliminate, the need for strong contractual shields against third country disclosure orders.

The thesis concludes that GDPR and AIA safeguards operate as a single, integrated compliance stack: when integrated into system architecture from day one, they allow Europe to participate fully in global AI research while preserving the fundamental rights standards distilled by *Schrems II.*

INTRODUCTION

Over the past decade, artificial intelligence (AI) has experienced unprecedented growth, transforming numerous industries and reshaping the global economy. Its success is powered in large part by the vast pools of data that fuel algorithms, enabling the development of increasingly sophisticated and accurate models which eventually leads to reliable AI systems. The demand for large, diverse datasets continues, as AI systems are being used more and more in areas like healthcare, finance, and transportation, among many others. In order to collect the amount and diversity of data required for effective AI innovation, businesses, researchers, and developers are forced, by this growing need, to look outside of their own borders.

However, this cross-border transfer of data brings with it significant legal and regulatory challenges, especially for organisations based in the European Union (EU). The EU's 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) imposes strict standards on how personal data is collected, stored, and shared, impacting the flow of information both within and outside EU's borders. While also having to take account of the EU's new Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (Artificial Intelligence Act/AIA), AI developers wanting to access global datasets have to manage a complicated dual framework of data protection requirements, Adequacy Decision, and contractual obligations. This environment can be very uncertain, making it more difficult to take advantage of the valuable global data required for dynamic research and product deployment.

Given the importance of data to AI development, understanding and resolving these legal complexities is crucial for EU-based businesses. By examining the complexity of cross-border data transfers and exploring potential frameworks for lawful and secure data exchanges, this thesis aims to highlight both the challenges and opportunities at the center of AI development and cross-border data transfer regulations. In doing so, it will shed light on how legislation and regulations shape the development of AI and the broader implications for data-driven progress in the EU.

The legal frameworks influencing any AI driven personal data flow out of the EU is outlined in Chapter 1. Adequacy Decision, standard contractual clauses (SCC), binding corporate rules (BCR), and the exporters obligation to ensure "essentially equivalent" protection are among the cross-border regulations outlined in the General Data Protection Regulation (GDPR). These are contrasted with the AIA, which risk-based framework overlays the GDPR with extra obligations for high-risk AI systems including bias testing, logging, security, and human oversight obligations that accompany the data wherever it travels. Despite the most recent EU-US Data Privacy Framework (DPF), the legality of cross-border transfers is still up in the air because *Schrems II* invalidated the EU-US Privacy Shield, which led the data protection authorities (DPAs) to introduce a "zero risk" standard. These provisions and case law combined, serve as a basis by which the rest of the thesis assesses the challenges in complying with the legislation and guidelines concerning cross-border data transfers for AI development.

Since a GDPR data protection impact assessment (DPIA) must first justify the transfer of personal data, followed by an AIA fundamental rights impact assessment (FRIA) that layers on bias testing, logging, and human oversight duties, Chapter 2 demonstrates that cross-border AI projects face a dual hurdle. This means that a lawful export alone is insufficient unless the two assessments are integrated throughout development and deployment.

Schrems II's invalidation of the EU-US Privacy Shield altered the circumstances in which cross-border data transfers may take place, but it did not mark the end of them. Chapter 3 examines how the CJEU, while preserving SCCs as a legitimate transfer tool, tightened the obligations for them post-*Schrems II.* It examines how the survival of SCC-based transfers depends on exporters proving through a transfer impact assessment (TIA) that the destination country's surveillance legislation, such as United States (US) FISA section 702, does not compromise EU level privacy and implementing supplementary measures, such as encryption or pseudonymisation. The EDPB's six step TIA method makes this a continuous, evidence driven obligation, as demonstrated by AI systems logs that must remain encrypted across borders or the transfer must be stopped.

When an AI system's data or operations leave the European Economic Area (EEA), Chapter 4 explains how the high-risk obligations of the AIA; documentation, automatic logging, and

human oversight, “follow” the system. It discusses how providers are required to maintain log files and technical files retrievable, and under EU-level security, even if they are located on foreign servers and are vulnerable to a third country discovery or surveillance legislation. Failure to do so results in non-conformity findings and the severe penalties imposed by the AIA. The chapter also points out how cross-border data governance is a key test of reliable AI since, in reality, exporting logs or documentation under post-*Schrems II* SCCs merely adds AIA obligations on top. While geography raises the risk of non-compliance, it never lessens the legal weight of these safeguards.

Chapter 5 assesses the fallback options remaining once SCC based transfers are strained and the DPF is under fire. The chapter shows that if the DPF or Adequacy Decision is struck down by either the Latombe (Case T-553/23) or the forthcoming *Schrems III* case, businesses will have to fall back on SCCs plus TIA. Only when exporters can prove that surveillance risks are still “essentially equivalent” to EU standards does post-*Schrems II* requirements permit such transfers. The AIA reinforces this risk-based proportionality test by requiring high-risk AI providers to maintain accessible logs, bias metrics, and human-oversight records wherever the data is stored.

Chapter 6 provides an overview of how cloud infrastructure is evolving into a forum for AI compliance. From 2025 the Data Act will add localisation and third country access restrictions, the draft of the Cybersecurity Certification Regime for Cloud Services points the same way. DPAs already interpret post-*Schrems II* requirements and “keep it in Europe” mandate, prompting hyperscalers, such as Microsoft, to launch sovereign clouds. The chapter highlights that technical separation may not provide the “essentially equivalent” protection demanded, explaining why such designs, as Microsoft's EU Data Boundary, appear to comply with EU traceability rules on paper but still struggle with US surveillance reach.

The Conclusion of the thesis knits together the arguments and analysis developed across the thesis and shows how they answer the posed research questions.

RESEARCH QUESTIONS

The main research question of the thesis is: To what extent does the combined GDPR-AIA regime govern cross-border transfers of personal data for development purposes of high-risk AI systems post-*Schrems II*?

In order to answer the main research question, three closely linked sub-questions help to guide the analysis in this thesis. These questions are:

1. How do the GDPR's data protection impact assessment and the AIA's fundamental rights impact assessment interact when a single data flow triggers both instruments, and where do their safeguards differ?
2. What legal weight does the AIA's documentation, logging, and human-oversight obligations have when the relevant records are stored or processed outside the EEA and become subject to third country surveillance or discovery powers?
3. Do standard contractual clauses, supported by transfer impact assessments and supplementary measures, still offer a legally sound and workable route for exporting data and AI logs to jurisdictions with similar surveillance laws to those critiqued in *Schrems II*?

When combined, these three lines of analysis show whether the post-*Schrems II* toolbox can still balance the protection of fundamental rights with the practical requirement for cross-border data flows in Europe's high-risk AI ecosystem.

METHODOLOGY

The thesis follows a doctrinal legal method with a single-country case study (the United States) to map the full compliance life cycle for cross-border data flows feeding high-risk AI operations. The doctrinal part answers the question "what is the law?". It systematically analyses the primary EU legislation (GDPR and AIA, and a mention of the new Data Act), the *Schrems II* judgement, and post-*Schrems II* soft law (EDPB, CNIL and European Commission) to find binding rules, close interpretive gaps and give guidance for further interpretation. The case study then tests those rules against the US jurisdiction that is condemned by *Schrems II* as not offering "essentially equivalent" EU level of protection. In addition, the thesis bases its privacy, data protection and redress standards on Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union.

The research questions, focused on legal overlap, cross-border enforceability and the validity of SCCs, are doctrinal by nature. Therefore, the doctrinal method is the most direct way to track rights, obligations, and enforcement mechanisms.

Because *Schrems II* was based on the incompatibility of US surveillance legislation with the EU fundamental rights standards, the US became the paradigmatic "problem" jurisdiction for the GDPR compliant data transfers. The thesis concentrates on the US jurisdiction as its primary third country case study, using the post-*Schrems II* EU-US data flows to demonstrate the wider legal and technical challenges that any cross-border data transfer outside the EEA now faces. Although concentration is in the US, the post-*Schrems II* requirements also apply to other third countries.

The thesis makes use of a small but expanding collection of peer-reviewed journal articles to place the legal-technical analysis of the thesis in the current academic debate. Since the academic conversation on post-*Schrems II* data transfers and AI compliance is still thin, every peer-reviewed source used in the thesis is recent, all falling between 2020 and 2024.

In addition, the thesis uses a concrete real life example by analysing Microsoft's EU Data Boundary (EUDB), which went into effect in February 2025. Examining the EUDB lets the analysis delve into concrete terms, whether localisation and encryption can effectively neutralise US surveillance powers and fulfill the post-*Schrems II* cross-border data transfer

requirements and AIA obligations. The information of the EUDB is gathered from Microsoft's own website.

Along with the materials introduced already, the thesis systematically reviews blog posts and websites from the NGO NOYB and EU institutions. This material is included for two methodological reasons, even though they are not considered as authoritative legal sources. First, in order to show how the GDPR-AIA requirements are operationalised by those who must advise or litigate on them, they provide current, practice oriented readings of court rulings and legislative drafts. Second, civil society remarks that may be under-represented in doctrinal literature are reflected by the NGO analyses, especially when it comes to implications for fundamental rights. Combining these viewpoints with academic and legal sources, enhances the assessment of the GDPR-AIA regime's governance on cross-border data transfers and highlights the viewpoints and possible biases present in non scholarly commentary.

1. LEGAL FRAMEWORK AND BACKGROUND

1.1 The General Data Protection Regulation

A defining feature of the GDPR's protection for EU citizens is that it covers personal data not only within the EU, but also provides safeguards when this data is transferred beyond EU borders.[1] This is relevant, as nowadays more and more services and products offered by firms based outside the EU are transferring personal data of the EU citizens to their servers, outside EU borders such as to the US.

The GDPR permits the transfer of personal data outside the EU or the EEA, under certain conditions.[2] Specifically, according to Article 44 of the GDPR, the exporter of the data bears the responsibility of ensuring that such transfers adhere to one of the legal bases established Articles 45-49 of the GDPR.[3]

The European Commission may decide that a third country offers an adequate level of protection. In this situation, personal data may be transferred to that country without further measures.[4] Data controllers are not required to put in place any extra protection measures in countries covered by an Adequacy Decision issued by the European Commission. Transfers to these jurisdictions are regarded as being exactly the same as transfers occurring inside the EU.[5] However, a transfer or series of transfers of personal data to a third country or an international organisation in the absence of an Adequacy Decision or suitable safeguards, may take place only in certain specific circumstances, such as a consumer's explicit consent or the necessity of data transfer for performing a contract with the consumer, may make the transfer permissible.[6]

In order to ensure appropriate safeguards, a data controller or processor may use standard contractiual clauses (SCCs) that have been adopted or approved by the European Commission, incorporating them into the contractual agreements with the recipient when

[1] Zac Amit et.al. 'The Court Speaks, But Who Listens? Automated Compliance Review of the GDPR', (Center for Law & Economics Working Paper Series, 01/2024, updated version March 2024), p.3.
[2] 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), [2016] OJ L 119, Chapter V.
[3] GDPR, art. 44.
[4] GDPR, *art. 45.*
[5] Zac et al., note 1, p.5-6.
[6] GDPR, art. 49(1)

transferring personal data to a third country.[7] Data transfers within a corporate group may also be lawful under binding corporate rules (BCRs), provided that a data protection authority has approved these rules for internal data exchange.[8]

1.1.1 Definitions

To make the context of the thesis easier to follow, here are some of the most often used GDPR terms in this thesis, as defined in Article 4 of the GDPR.

Personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[9]

Pseudonymisation is "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."[10]

Controller is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."[11]

Processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". [12]

[7] GDPR, art 46(2)(c), (d).
[8] GDPR, art 47.
[9] GDPR, art. 4(1).
[10] GDPR, art. 4(5).
[11] GDPR, art. 4(7).
[12] GDPR, art. 4(8).

1.2 The Artificial Intelligence Act

The Artificial Intelligence Act (AIA) is a risk-based framework to regulate the development, deployment, and use of AI technologies. It aims to establish a uniform set of rules for AI technology used in the EU in order to guarantee that these systems are trustworthy, and compliant with current legislation and principles, including privacy and fundamental rights.[13]

The AIA classifies AI systems into different risk categories based on the potential harm they can cause. The purpose of these risk groups is to regulate AI in proportion to the risks they pose. The categories are unacceptable risk, high-risk, limited risk, and minimal or no risk AI systems. This thesis is particularly focused on the AI systems belonging to the high-risk group.

The Recital 27 of the AIA explains that a trustworthy AI system is human-centric, protects health, safety and fundamental rights while meeting seven ethical requirements; human oversight, technical robustness, privacy and data governance, transparency, diversity and fairness, societal and environmental well-being, and accountability.[14] The requirements for trustworthy AI are laid out in Section 2, Articles 9-15,[15] and opened up below.

Providers must ensure that all data regardless of origin, complies with the AIA standards when high-risk AI systems use cross-border data sets, such as training data from non EEA sources. This can include robust data governance measures, bias detection, and documentation requirements. In order to ensure lawful and transparent data handling, organisations importing or exporting data must also comply with relevant data transfer rules under current regulations, such as the GDPR.[16]

Providers are required to map and address potential risks related to data use, including any risks specific to international transfers, such as those concerning data privacy, security, or surveillance concerns outside the EU, in accordance with the requirements for risk

[13] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), [2024] OJ L 1689
[14] Artificial Intelligence Act, Recital 27.
[15] Artificial Intelligence Act, Section 2.
[16] Artificial Intelligence Act, art. 10.

management systems and human oversight.[17] In practice, meaningful human oversight requires human operators to monitor the system and, if needed, adjust or deactivate it. When an AI system demonstrates unexpected or unsafe behaviour, providers should make sure that the people in charge of supervision have the necessary resources, authority, and training to step in. In order for operators to take action in the event that there are problems related to data security or integrity in another jurisdiction, the mechanisms may also require clarification on how data is handled across borders.[18]

Both Articles 11 and 12 require detailed logs and records of the developing, training, and use of AI systems. Providers must provide documentation of how data transfers adhere to GDPR or other relevant privacy and cybersecurity regulations if any part of the training or operation involves data moving into or out of the EU.[19] Maintaining accurate records is essential as authorities may request proof that cross-border flows are lawful and do not undermine the safety, reliability, or fundamental rights protections central to the AIA.[20]

Given the differences in legal and technical standards between jurisdictions, cybersecurity measures become especially relevant when data is transferred internationally. Compliance requires AI systems to be resilient to threats in different data environments. Therefore, providers must anticipate and reduce any additional risks or complications that may arise from processing and storing data outside of the EU.[21]

1.2.1 Definitions

To make the context of the thesis easier to follow, here are some of the most often used AIA terms in this thesis, as defined in Article 3 of the AIA.

AI system is “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments”.[22]

[17] Artificial Intelligence Act,,art. 9.
[18]Artificial Intelligence Act, art. 14.
[19] Artificial Intelligence Act, art.11.
[20]Artificial Intelligence Act, art.12.
[21]Artificial Intelligence Act, art.15..
[22]Artificial Intelligence Act art 3(1).

Provider is "a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge".[23]

Deployer is "a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity".[24]

Importer is "a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country".[25]

Operator is "a provider, product manufacturer, deployer, authorised representative, importer or distributor".[26]

Market surveillance authority is "the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020". [27]

1.3 Cross-Border Data Transfers Post-Schrems II

In its significant case of Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems C-311/18 (*Schrems II)*, the CJEU reshaped the regulatory structure for transferring personal data from the EEA to third countries.[28] The CJEU ruled that US surveillance laws and practices did not comply with the GDPR's data protection requirements, invalidating the EU-US Privacy Shield. This is because the surveillance programmes are not limited to what is strictly necessary and proportionate.[29] In addition, they offer no judicial redress equivalent to Article 47 of the Charter of Fundamental Rights of the

[23] Artificial Intelligence Act, art 3(3).
[24] Artificial Intelligence Act, art. 3(4).
[25]Artificial Intelligence Act, art. 3(6).
[26]Artificial Intelligence Act, art 3(8).
[27] Artificial Intelligence Act, art 3(26).
[28] Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. C-311/18.
[29] Fahey Elaine. 'Strategic Litigation and EU Law on Cross-Border Data Transfers: On the Place of EU Law in the Work of Schrems and NOYB', (Nordic Journal of European Law, Volume 7, Issue 4, 2024) p. 141.

European Union (Charter).[30] In contrast, the CJEU upheld that the standard contractual clauses (SCCs) can provide "essentially equivalent" protection for transfers of personal data, when combined with suitable supplementary measures,[31] in addition with appropriate assessments discussed in Chapters 2.2 and 3.2.

The judgement resulted in the EU data protection authorities (DPAs) to develop a strict "zero risk" approach in relation to Chapter V of the GDPR, meaning that when transferring personal data outside of the EU, data controllers and processors are required to eliminate any possibility of unauthorised access by foreign law enforcement agencies or intelligence body in nations lacking EU equivalent data protection safeguards. This also applies to other countries than just the US, even though practically all the enforcement actions issued by the EU DPAs have involved transfers to the US.[32] However, as discussed in Chapter 5.2, this "zero-risk" approach is unrealistic and almost impossible to achieve in practice.

The European Data Protection Board (EDPB) released guidelines in response to *Schrems II* on how to assess the adequacy of third country legislation[33] and on implementing protective measures in place to preserve an "essentially equivalent" EU level of data protection.[34] Despite continuous attempts to improve data transfers between the EU and the US using frameworks such as the new EU-US Data Privacy Framework (DPF), which was specifically created as a result of the *Schrems II* ruling, legal uncertainties remain. The compliance of third country surveillance laws with the GDPR's fundamental rights standards is still being closely examined by courts and regulatory bodies, and it is not impossible that more challenges to the current or future frameworks will arise.[35] This matter will be further discussed in Chapter 5.

[30] Gulbakyt Bolatbekkyzy. 'Legal issues of cross-border data transfer in the era of digital government', (Journal of Digital Technologies and Law, 2024), p.297.
[31] C-311/18, note 28, paras 134 and 148.
[32] Christakis Theodore. 'The Zero Risk Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach', (Centre for Information Policy Leadership, Cross-Border Data Forum, February 2024), p. 11-12.
[33] EDPB. 'Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework', (Version 1.1, Adopted on 4 November 2024)
[34] EDPB. 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data', (Version 2.0, Adopted on 18 June 2021)
[35] Giovanni Tricco. 'The New Transatlantic Data Agreement Placed in Context: Decoding the Schrems Saga within the Digital Economy', (Journal of Law, Market & Innovation, Vol 3 - Issue 1/2014), p.108-110.

1.3.1 Supplementary Measures

Exporters who use standard contractual clauses (SCCs) or any other GDPR Article 46 tool, are required by the EDPB's Recommendations 01/2020 (v 2.0) to add supplementary measures when needed to raise protection to a level that is "essentially equivalent" to the EU level of protection. Those measures are separated into three categories under the recommendation's Annex 2.[36]

Technical measures make foreign authorities unable to access the data technically. For example, transport layer or end to end encryption with EU only key control, which allows the provider overseas to store payload but never decrypt it. Another example is pseudonymisation, which renders any data seized outside the EEA useless without the EU held key.[37]

Using additional contractual measures, the importer provides the exporter with legally binding promises that support the SCCs, it forbids back-doors, promises to oppose or resist orders for disproportionate disclosure, gives the exporter access to tamper-proof logs and short notice audit rights, and commits to maintaining agreed upon technical measures, such as encryption, or promptly informing the exporter of any new law enforcement demand.[38]

Organisational measures are internal policies that integrate privacy governance into daily operations, such as detailed encryption key management and incident response plans, and strict role based access controls. They also include a dedicated government request team that is trained to examine and, when necessary, challenge access requests, and frequent staff training on EU fundamental rights standards to help staff identify and escalate problematic requests.[39]

The EDPB's Recommendation emphasises that exporters must combine and document whichever organisational, contractual, and technical measures successfully eliminate the particular surveillance risks identified for their transfer, as no single measure is necessarily automatically sufficient. However, the list of these measures is not exhaustive, there is room

[36] EDPB, note 34, Annex 2.
[37] *Ibid,* Annex 2, Use Cases 1-3.
[38] EDPB, note 34, Annex 2, paras 98-105.
[39] *Ibid,* Annex 2, paras 128-131.

for developments, such as technical or legal. The transfer must be halted or avoided completely if no combination is able to accomplish that objective.[40]

1.3.2 Adequacy Decision and the EU-US Data Privacy Framework

European Commission adopted the Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (Adequacy Decision).

According to the Adequacy Decision, the US provides an adequate degree of protection for businesses on the Data Privacy Frameworks (DPF) list under Article 45 GDPR.[41] This turns the DPF into an automatic legal basis for data transfers from the standpoint of an EU controller, as any listed US company may receive personal data without further paperwork.

The DPF, in summary, is a US self certification program administered by the Department of Commerce. Any US organisation that is subject to the Department of Transportation's or the Federal Trade Commission's investigatory powers may voluntarily certify that it will adhere to the DPF principles. The organisation's name is added to a public Data Privacy Framework list once the Department reviews the application, after that the principles become enforceable under US law.[42] The principles apply to all EU personal data that a listed company gets, even after it exits the program. The principles replicate the core GDPR rules, such as data minimisation, accuracy, and purpose limitation.[43]

To conclude, the DPF provides for the rule book for the US companies to follow, while the Adequacy Decision turns that rule book into a kind of a "passport" that lets EU data flow to any business which has its name on the DPF list.

---

[40] *Ibid,* note 34, Annex 2, paras 74-76.
[41] Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, [2023] OJ L 231
[42] *Ibid,* Recitals 28, 45, 48.
[43] Commission Implementing Decision EU 2023/1795, Recitals 13 and 63.

2. THE INTERACTION BETWEEN THE GDPR AND THE AIA ON CROSS-BORDER DATA TRANSFERS

The rapid development of AI over the past years has compelled businesses to look for larger and more varied datasets, often from sources beyond national borders. However, EU-based businesses must navigate with a dual regulatory environment: the AIA adds new requirements to ensure trustworthy AI development and use, while the GDPR sets stringent standards for the cross-border transfer of personal data.

It is important to note, that the GDPR's provisions on cross-border data transfers are not overridden by the AIA. Rather, the AIA introduces complementary requirements relating to cybersecurity, risk assessment, documentation, and data governance, which are applicable regardless of the origin or destination of the data. Consequently, when designing and operating high-risk AI systems, providers must effectively address cross-border data flows in order to ensure compliance with both the AIA and EU data protection legislation. The thesis will further explore these requirements in later chapters.

Examining the ways in which the GDPR and the AIA interact, helps to clarify the opportunities and pitfalls of AI-driven innovation in the EU, and offers a road map for businesses attempting to effectively and responsibly handle cross-border data flows.

2.1 Overlap in Scope

It is not uncommon for personal and non-personal data to be processed together, for example for AI training purposes. According to the European Commission, "if the non-personal data part and the personal data parts are 'inextricably linked', the data protection rights and obligations stemming from the General Data Protection Regulation fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset".[44] This reinforces the need for providers to apply the GDPR's safeguards even in seemingly anonymised or mixed datasets, specifically when these are transferred across borders. More on this subject is covered in Chapter 3.2.1, which looks at the types of personal data that can be found in AI logs.

[44] COM/2019/250 final, p.9.

Although both the GDPR and the AIA offer numerous opportunities for collaboration, centering on identifying and classifying high-risk activities, their scopes and enforcement mechanisms differ. The GDPR gives Member States and EEA nations the authority to list processing operations that require data protection impact assessment (DPIA), which will be discussed later in the chapter. This means that situations in which AI systems utilise personal data, shall be governed by both the GDPR and the AIA. Whether such systems qualify as high-risk, will ultimately depend on both the regulations.[45] As a result, businesses governed by both regulations, face heightened compliance complexity.

Even while the usage of AI systems handling personal data is expanding quickly, the AIA does not specify how its obligations relate to those of the GDPR or provide a structure for collaboration between their authorities. This overlap might result in uncertainty, slowed enforcement, and increased financial hurdles to innovation, if not resolved.

Moreover, despite the GDPR being already enforced for some years, no thorough analysis of the various DPIA requirements across the EU has been conducted.[46] Since DPIAs are usually used in the early stages of AI training, as discussed in the next sub-chapter, this lack of clarity leads to inconsistent AIA implementation. As a result businesses have the ongoing need to ensure that AI systems are updated and flexible enough to accommodate shifting societal viewpoints, while trying to figure out which AI applications qualify as high-risk under each nations data protection rules.[47]

2.2 Relationship Between Data Protection Impact Assessment and Fundamental Rights Impact Assessment

The practical overlap of the two impacts becomes clearer when comparing them. They come into play in different stages of an AI project. The GDPR requires a data protection impact assessment (DPIA) to be carried out before processing personal data that "is likely to result in a high risk to the rights and freedoms of natural persons".[48] Additionally, Article 35(11) of the GDPR mandates that the controller review and update the DPIA whenever processing

[45] Rintamäki Tytti, et al.'High-Risk Categorisations in GDPR vs AI Act: Overlaps and Implications', (ADAPT SFI Research Centre at Dublin City University and Trinity College Dublin,Volume 11, 2023), p. 2-3.
[46] *Ibid,* p. 2-3.
[47] Kokoulina Olga. 'Challenges in Digital Compliance: Risk Assessment and Fundamental Rights under the GDPR and the EU AI Act', (Paper presented at Processes, Laws and Compliance workshop at the 6th International Conference on Process Mining, University of Copenhagen, 2024), p.2.
[48] GDPR, art 35 (1).

operations, or the risk associated with the changes.[49] The DPIA may need to be reviewed multiple times during development, because model-training pipelines often incorporate new datasets, or broaden the geographic scope long before the product is released.

By contrast, the AIA's Fundamental Rights Impact Assessment (FRIA) is required when assessing high-risk AI systems.[50] It is focused on mitigating the potential risks to health, safety, and fundamental rights linked to these high-risk systems. Market placement happens late in the life cycle of an AI system, after the design and intended use time is settled.

Consequently, a single cross-border AI project may undergo several DPIA rounds during the development stage, followed by a final FRIA that combines the earlier findings while incorporating the AIA's AI specific safeguards, such as bias testing, robustness checks, logging, and human oversight.

The AIA permits the reuse or adaption of previous DPIAs to fulfill FRIA criteria.[51] This eliminates having to do the same work again, and it encourages uniformity in compliance by allowing risk evaluations to be carried out also during AI development, to be incorporated into the final FRIA. Collaboration and knowledge sharing are essential throughout the AI systems lifecycle.

To conclude, it is clear that the GDPR and the AIA both offer a framework for classifying activities as high-risk, requiring that their impacts on rights and freedoms be evaluated using the DPIA and FRIA as tools.

2.3 Divergences in Cross-Border Compliance

When a cross-border transfer is examined under both GDPR and AIA (and DPIA and FRIA), they begin to divide in four fundamentally significant areas, although still having plenty in common.

According to Article 35 of the GDPR, the controller must identify the Chapter V transfer mechanism and specify the legal justification for each processing purpose laid out in Articles

[49] GDPR, art 35(11).
[50] Artificial Intelligence Act, art 27.
[51] Artificial Intelligence Act, art. 27(4).

6 or 9 of the GDPR.[52] FRIA template only considers the impact of the AI system on fundamental rights, it does not include any parallel requirements.[53] Meaning that only DPIA asks on what legal basis may the data travel.

Both the GDPR and the AIA apply to high-risk AI projects that transmit training data outside of the EEA. A comparative study found that of the 25 AIA's Annex III high-risk scenarios, 23 already fall under DPIA triggers, and the remaining may do so based on the involvement of personal data in those cases.[54] This means that a DPIA does generally become necessary whenever an AI system processes personal data, as personal data is usually involved from the earliest stages of AI development. Versus FRIA, that involves both personal and non-personal data, because the AIA has a broader material scope. Therefore, a DPIA may be needed well before the final AI product reaches the market.

Any threat to a natural person's "rights and freedoms" including financial loss, damage to one's reputation, and other interests, is measured by the DPIA.[55] As mentioned before, the FRIA is interested in only fundamental rights violations acknowledged under EU legislation. Therefore, different mitigation criteria may result from the same transfer receiving a higher risk score under the GDPR than under the AIA.

Controllers and processors are required by Article 32 of the GDPR to implement "appropriate technical and organisational measures".[56] The regulation purposely frames the list of safeguards, in that article, as illustrative rather than exhaustive, by using the wording "inter alia".[57] Because of this, the list is open ended, leaving the controller to determine, case by case, which instruments are the most sufficient to use.

[52] GDPR, art. 35.
[53] Pandit Harshvardhan J., Rintamäki Tytti. 'Towards An Automated AI Act FRIA Tool That Can Reuse GDPR's DPIA', (Presented at CLAIRvoyant (ConventicLE on Artificial Intelligence Regulation) Workshop 2024), p.2-4.
[54] Rintamäki, note 45, p.4-5.
[55] GDPR, art. 35 together with recital 75.
[56] GDPR, art. 32.
[57] GDPR, art 32.

By contrast, AIA has a set of AI specific obligations, such as post-market monitoring,[58] bias testing,[59] logging,[60] and human oversight design.[61] The last two are discussed in more detail in chapters 4.2.2 and 4.2.3. Therefore, bias metrics or human oversight techniques may still be necessary to meet the FRIA, for a log file that is legally encrypted and transferred under the GDPR.

Even if a controller exports AI system logs lawfully under the GDPR (by using post-*Schrems II* standard contractual clauses (SCC) and encryption that complies with Article 32 of the GDPR), if the logs are not integrated into the AI system's workflow for bias detection, traceability, and human oversight, the provider may still violate the AIA. Only when logs are automatically generated and stored, organised so they can be used for bias and robustness testing, can be reviewed by qualified humans who can intervene, and support a life cycle post market-monitoring plan, do high-risk systems qualify as compliant under the AIA. Even though the cross-border transfer itself satisfies the GDPR requirements, the system fails the AIA's conformity test if the exported logs are stored in a vault abroad in a third country that is unable to provide these functions. This shows that while the GDPR establishes a flexible security baseline, the AIA adds required AI specific safeguards that must also be met.

After analysing how the GDPR's data protection impact assessment (DPIA) and the AIA's Fundamental Rights Impact Assessment (FRIA) overlap in their roles in managing risks associated with cross-border high-risk AI projects, it is equally important to take into account the transfer impact assessment (TIA), which is essential for guaranteeing compliance to post-*Schrems II* cross-border data transfer requirements. Notably, the DPIA, which, as mentioned before, assesses risks to data subjects from processing activities likely to result in high risk, cannot substitute the TIA, which specifically evaluates risks to the EU level of protection caused by transfers to non-adequate countries before exporting personal data. The following chapter will explore how TIA functions, and how it complements the DPIA and FRIA.

[58] Artificial Intelligence Act, art Art. 72 (and cross-references in Art. 12 (2)(b) & Art. 73)
[59] Artificial Intelligence Act, Art. 10(2)–(4); Recitals 69–70.
[60] Artificial Intelligence Act, art 12.
[61] Artificial Intelligence Act, art 14.

3. STANDARD CONTRACTUAL CLAUSES POST-SCHREMS II

Building on the understanding of the interaction between the frameworks of the GDPR and the AIA, as well as the complementary functions of the DPIA and FRIA in managing risks associated with high-risk AI, it is now necessary to examine the specific legal mechanisms that facilitate cross-border data transfers within this regulatory environment.

Standard contractual clauses (SCC) were maintained as a valid transfer mechanism by the CJEU, albeit with some changes, their use is now subject to additional requirements: SCCs set stricter requirements for data importers and clarified responsibilities in areas such as government access requests.[62] Businesses are now required to conduct transfer impact assessments (TIA) to determine whether the importing jurisdiction's laws and practices comply with the protections provided by the GDPR. As discussed in Chapter 1.3.1, to ensure that data remains as secure abroad as it would within the EEA, exporters must implement supplementary measures in place, such as technical, contractual or organisational measures, when significant risks are identified. These measures include encryption and pseudonymisation.

Therefore, it is necessary for both data importers and exporters to assess whether taking additional steps can significantly lower those risks. Because, if the laws and practices of the third country of the destination prohibit the data importer from adhering to the SCCs and the "essentially equivalent" EU level of protection, then the transfer and processing of personal data under those clauses should not take place.[63] This applies particularly to third countries that have extensive surveillance regimes, like the US.

Safe Harbour[64] and its successor Privacy Shield[65] were both invalidated, because in both cases the CJEU determined that the corresponding adequacy decisions had to be annulled because the expansive US surveillance laws along with the absence of independent and

[62] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, [2021] OJ L 199
[63] *Ibid,* recital 19.
[64] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7.
[65] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1.

effective redress under Article 47 of the Charter, violated EU fundamental rights standards.[66] A thorough, adequacy level framework for regular transatlantic data transfers is still lacking between the EU and the US, despite stricter post-*Schrems II* SCCs that include mandatory TIAs and strong supplementary measures.

The EU-US Data Privacy Framework (DPF) is the third attempt, after Safe Harbour and the Privacy Shield, but it only provides a limited avenue for EU citizens to seek redress through the EO 14086, and largely preserves the US mass surveillance powers under the Foreign Intelligence Surveillance (FISA) section 702 and EO 12333.[67] These deficiencies have already led to two annulment actions: the upcoming *Schrems III* challenge, which NOYB made a public announcement of,[68] and MP French Philippe Latombe's Case T-553/23,[69] both will be analysed in Chapters 5.1 and 5.2 of this thesis.

3.1 US Surveillance Concerns

The Executive Order (EO) 14086 was published in October 2022, its aim is to strengthen protections for US signals intelligence operations, especially with regard to transatlantic data transfers under the EU-US Data Privacy Framework (DPF). The EO 14086 introduced stricter limitations on surveillance, which expressly prohibits data collection aimed to target protected groups, suppressing dissent, or political opinions. It requires intelligence operations to be proportionate, necessary, and targeted at validated priorities.[70]

Additionally, it created a two tiered redress mechanism, replacing the Privacy Shield mandated Ombudsperson with a Civil Liberties Protection Officer (CLPO) and a Data Protection Review Court (DPRC), thereby providing independent oversight of complaints.[71] Despite these advancements, there are still issues regarding the EO 14086's complete compliance with EU data protection standards, as it still allows for bulk data collection and gives the US authorities broad discretion.[72] However, there has been a significant shift in the

---

[66] Fahey, note, 29, p. 131-132.
[67] Connolly Matthew. 'WILL THE EU-US DATA PRIVACY FRAMEWORK SURVIVE SCHREMS III?', (Trinity College Law Review, Volume 27, 2024, pp. 87-124.), p.123-124.
[68] NOYB. 'European Commission gives EU-US data transfers third round at CJEU', (NOYB, 10 July 2023) Available online: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu?utm_source=chatgpt.com (23.4.2025)
[69] T-553/23 Latombe v Commission [2023] OJ C/2023/348
[70] Connolly, note 67, p.106-111.
[71] Commission Implementing Decision EU 2023/1795, Recital 204.
[72] Connolly, note 67, p.106-111.

oversight, highlighting that the situation is no longer as stable as it was when issuing the EO 14086, this will be discussed in more detail in Chapter 5.1 and 5.2.

In practice, demonstrating that supplementary measures fully eliminate legal concerns is difficult and often impossible in jurisdictions with surveillance frameworks similar to those denounced in *Schrems II.* "Often impossible", because the EDPB leaves room for transfers if strong technical measures can neutralise foreign law access, such as end to end encryption.

Good examples of problematic surveillance frameworks include bulk, indiscriminate collection of data and information under the Foreign Intelligence Surveillance Act (FISA) section 702 or EO 12333, which permits US intelligence agencies to obtain data from providers. Such practices are not "essentially equivalent" to the protections guaranteed by the Articles 7, 8, and 47 of the Charter of Fundamental Rights of the European Union (Charter).[73] In these cases, the GDPR requires the data exporter to withhold or suspend the transfer even if SCCs have been signed.

Unfortunately, the surveillance powers that invalidated the former Privacy Shield have not vanished. In fact, they are even more relevant to all EU-US transfers due to developments post-*Schrems II.* The core protection gaps stem from US national security authorities' operations, which interfere with fundamental EU rights. Together with the abovementioned interference with the EU Charter rights, and the fact that the CJEU noted in its *Schrems II* judgement that "it is common ground that those clauses are not capable of binding the authorities of that third country, since they are not party to the contract"[74], the SCCs are unable to make up for the shortcomings in the degree of protection provided by US law, and in any other similar jurisdiction.[75]

That fundamental defect now has a wider legal significance because the US Congress reauthorised FISA section 702 in April 2024, expanding the definition of "electronic communication service provider", meaning that it could include cloud platforms, and data centre hosts who may be required to assist surveillance operations.[76]

---

[73]Connolly, note 67, p.100.
[74] C-311/18, paragraph 125.
[75] Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation, section 7.160, p. 92.
[76] H.R.7888 - Reforming Intelligence and Securing America Act,118th Congress (2023-2024), Sec. 24.

Taken together, the US surveillance concerns, identified in *Schrems II,* remain alive. Therefore, both the importer and the exporter must "warrant that they have no reason to believe" that local law will prevent the importer from respecting the SCCs.[77] That commitment needs to be documented, and the document for that is TIA.

3.2 Transfer Impact Assessment

A transfer impact assessment (TIA) obligates the exporter, according to France's data protection authority, Commission Nationale Informatique & Libertés (CNIL), to evaluate the degree of the third countries ability to uphold the safeguards and the need for additional safeguards before using the transfer tools specified in Articles 46(2) and 46(3) of the GDPR.[78]

With an emphasis on how public authorities might access the data, it accomplishes this by comparing EU standards with the laws and actual government access practices of the destination country. The TIA must demonstrate whether supplementary, technical or organisational, measures can restore EU equivalent protection if gaps are found. If not, the transfer should not proceed. The importer must provide complete, concrete information rather than merely an executive summary since it controls a large portion of the evidence, including details of local law enforcement demands and system architecture. As part of the relationship between a controller and a processor, the processor's obligation is to transmit this information to the controller under the GDPR's Article 28(3)(h).[79] In addition, the depth of those checks should scale with the potential impact on data subjects' rights and freedoms..[80]

Following *Schrems II*, exporters were instructed by the European Data Protection Board (EDPB) to "verify, on a case-by-case basis", if the third country environment compromises the selected transfer instrument and, if so, to implement supplementary measures or stop the transfer.[81]

---

[77] Commission Implementing Decision (EU) 2021/914, Clause 14(a).
[78] Commission Nationale Informatique & Libertés. 'Practical Guide Transfer Impact Assessment', (Final version, January 2025), p. 3-7.
[79] *Ibid*, p. 3-7.
[80] Commission Nationale Informatique & Libertés, p. 9.
[81] C-311/18, recital 134.

The *de facto* framework for TIAs is a six step methodology that was established by the EDPB.[82] Organisations must first list all personal data flows out of the EEA and make sure that each item is absolutely required for its intended use. Second, they decide on a legal transfer mechanism, such as an EU Adequacy Decision, if one exists or in the absence of one, an Article 46 of the GDPR tool, such as standard contractual clauses (SCCs) or binding corporate rules (BCRs). [83]

Third, they conduct a TIA, analysing whether the laws of the destination country, specifically its surveillance capabilities, could compromise that instrument. Fourth, they implement supplementary, organisational, contractual, or technical safeguards to close any gaps and restore protection equivalent to EU standards. If none of these measures are successful, the transfer must stop.[84]

Fifth, it is necessary to finish any formal actions that are prompted by those safeguards, such as updating contract annexes. Lastly, since regulators have the authority to stop transfers as soon as that requirement is no longer fulfilled, exporters must continuously verify and record that the protection is still "essentially equivalent" to the EU standards.[85]

The TIA falls in between the data protection impact assessment (DPIA) and fundamental rights impact assessment (FRIA), in terms of placement and the relationship between all of the three risk assessments. The TIA compliments DPIA by focusing on cross-border data transfers at the moment they are planned, kicking in before the data is transferred. Its results are then incorporated into the final FRIA, which complements all previous risk assessments and adds the AI specific safeguards, such as logging, and human oversight, required for placing the system on the EU market.

3.2.1 AI Logs and Personal Data - Surveillance Risk

Due to the AIA's reliance on GDPR compliant exports for logging, an AI provider's compliance path is directly influenced by these elevated standard contractual clause (SCC) duties. Though with a technical twist, AI system logging presents the same cross-border risk

[82] EDPB Recommendations 01/2020, Version 2.0, p.2-3.
[83] *Ibid*, p 2.
[84] EDPB Recommendations 01/2020, Version 2.0, p.3-4.
[85] EDPB Recommendations 01/2020, Version 2.0, p.3.

that alarmed the CJEU in *Schrems II*. Taken together, the EDPB's Opinion 28/2024[86] on Certain Data-protection Aspects of AI Models shows that a single training log file can simultaneously capture three different classes of personal data.

It may store direct identifiers, for example a customer service AI system can be trained based on "historical conversation data to provide responses to user queries",[87] and in some cases it can be refined on a person's voice recordings.[88] These logs also frequently record indirect identifiers, such as IP addresses (which can single someone out when combined with other data). This kind of data is considered to be personal data after a CJEU judgement under the GDPR's Article 4(1), as they allow for the "direct or indirect" identification of a natural person.[89]

Lastly, from those same interactions, the AI model itself can produce behavioural profiles and other conclusions about the user. The same EDPB's opinion emphasises that many models are specifically made to infer such characteristics. Sometimes the models can "reveal" or regenerate training data meaning that these kinds of models are not anonymous.[90]

Because third country surveillance powers, such as US' FISA section 702, is technology neutral, its intelligence agencies could compel access to these logs just as readily as to an ordinary customer database.[91] Therefore, a GDPR compliant Transfer Impact Assessment (TIA) must thoroughly examine the logging pipelines[92].

The data elements should be mapped, and then decided which parts of the logs are personal data. When evaluating risk, the exporter must treat embedded data and gradient updates as personal data since they can be traced back to a user.[93] The government access risk should be

---

[86] EDPB. Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (Adopted on 17 December 2024)
[87] *Ibid*, para 22.
[88] EDPB Opinion 28/2024, para 29.
[89] Patrick Breyer v Bundesrepublik Deutschland, C-582/14, para 65(1)
[90] EDPB Opinion 28/2024, paras 29 and 31.
[91] Tricco Giovanni.'The New Transatlantic Data Agreement Placed in Context: Decoding the Schrems Saga With the Digital Economy', (Journal of Law, Market & Innovation, Volume 3, Issue 1/2024), p. 99-100.
[92] The definition by Squark:"An AI Pipeline is an end-to-end construct that orchestrates data flow into, and output from, a machine learning model (or set of multiple models). The pipeline includes the raw data input from the source, features, outputs, the machine learning model and model parameters, and other prediction outputs" Available online: https://squarkai.com/whats-an-ai-pipeline/#:~:text=An%20AI%20Pipeline%20is%20an,parameters%2C%20and%20other%20prediction%20outputs. (17.5.2025)
[93] EDPB Recommendations 01/2020, paras 80-83, p. 23-24.

also taken into account and be analysed as explained in Chapter 3.1. Despite stating otherwise in the SCCs, the importer may be legally compelled to disclose the logs if the cloud storage where they are stored is located in a jurisdiction where the mass collection orders are permitted. Moreover, as per Chapter 3.2, the exporter must presume that contractual guarantees alone are insufficient in cases where the destination country lacks clear and effective remedies for EU data subjects, as the CJEU discovered with regard to US intelligence legislation.

It is only after this legal-technical reality check that the exporter can determine whether supplementary measures will close the gap. A solution could be, for example, encrypting logs from beginning to end with decryption keys stored only in the EEA or, if workflow permits, storing raw logs in the EU exclusively.

The transfer may proceed under SCCs if such measures make the data incomprehensible to foreign authorities, otherwise, it must be paused. To put it briefly, applying post-*Schrems II* requirements to AI logging entails demonstrating through a detailed, evidence backed TIA that the risks associated with surveillance legislation have been technically neutralised before any personal data is allowed across the border.

4. OBLIGATIONS FOR CROSS-BORDER DATA FLOWS IN AI

4.1 Cross-border Data Flows for AI Development

Cross-border data flows are fundamental for building trustworthy AI systems. Innovations in AI rely on the exchange of resources and knowledge across borders, which specifically entails sharing a variety of datasets that are impossible for one single nation to produce on its own. The necessity of these flows clarifies why the legal weight of AIA's obligations across borders matters. However, those flows work only when they are supported by harmonised regulations, and solid data protection safeguards. The ability to make data globally available and responsibly governed will be crucial to the development of AI in the (near) future.[94]

4.2 The Weight of AIA's High-Risk Obligations Outside of the EEA

Post-*Schrems II*, controllers primarily rely on standard contractual clauses (SCC) along with the supplementary measures to export logs and documentation. The following sections demonstrate why those exports continue to be subject to the cross-border obligations imposed by the AIA.

AIA's obligations do not lose their weight merely because they are executed outside the EEA, rather they "travel with the system". Article 2(1) read in conjunction with Recital 21 and 22 guarantees "level playing field and an effective protection of rights and freedoms of individuals across the Union" by making it clear that the AIA applies "in a non-discriminatory manner, irrespective of whether they are established in the Union or in a third country".[95] Performing actions on servers or workstations located in a third country does not lessen their legal weight, on the contrary, it only increases the provider's compliance risk in the event that a foreign surveillance legislation compromises the confidentiality, availability, or integrity of the records at the EU level.[96]

Documentation, logging, and human oversight inputs are considered inflexible compliance instruments by the AIA, because they provide the audit trail and traceability that regulators require for conformity assessment and post market enforcement. Therefore, an AI system that

[94] Kseng San. 'International Collaboration in AI Research and Development', (International IT Journal of Research, Volume 2, Issue 1, Jan-March 2024), p. 1-5.
[95] Artificial intelligence Act, Recital 21.
[96] Artificial intelligence Act, Recital 22.

does not have these features is not permitted to be sold in the EU. Furthermore, moving the systems outside of the EEA carries the AIA with them, the obligations retain their full legal force, and any weakening resulting from foreign surveillance or discovery is the businesses responsibility to address rather than a legal loophole in EU law.

4.2.1 Documentation

Before being placed on the market, Article 11 of the AIA requires providers to create a single, comprehensive file that includes at least all Annex IV elements of the AIA, and demonstrates how the system meets all substantive requirements.[97] In addition, Article 18 of the AIA requires the provider to keep the file accessible to national authorities for ten years after the AI system is put on the market, without a specific mention of the country, server, or cloud the system is located in. The only requirement is that it be "at the disposal" of EU regulators.[98]

The documents can thereafter be obtained "upon a reasoned request" by any competent body under Article 21 of the AIA.[99] The provider simply breaches the cooperation duty and runs the risk of enforcement if a location outside the EEA, foreign discovery order, or state surveillance statute hinders quick delivery, meaning that geography gives no safe harbour. Article 22 of the AIA mandates the appointment of an authorised representative in the EU who maintains a copy of the technical documentation and is able to deliver it upon request in order to guarantee access even in cases where a provider is located outside the EEA.[100]

4.2.2 Logging

The AIA's main traceability tool for high-risk systems is logging (automatic recording). Its force is unaffected by a server located outside of the EU. Providers are required, by Article 12 of the AIA, to incorporate logging procedures into systems that will automatically record events that are relevant to risk assessment and compliance.[101] According to Article 19(1) of the AIA, those logs must be kept for a minimum of six months, or a time frame suitable for the high-risk AI system's intended use.[102]

---

[97] Artificial intelligence Act, art 11.
[98] Artificial intelligence Act, art. 18.
[99] Artificial intelligence Act, art 21.
[100] Artificial intelligence Act, art 22.
[101] Artificial intelligence Act, art 12.
[102] Artificial intelligence Act, art 19 (1).

The provider is required to make the logs available "upon a resonated request by a competent authority", even if the archive of logs is stored in a third country cloud.[103] Additionally, market surveillance authorities have the right to request remote access or the actual raw records, according to Article 74(12) of the AIA.[104]

Therefore, cross-border storage increases risk rather than reduces it. If disclosure is delayed or distorted by foreign discovery rules, surveillance requirements, or technical obstacles, the system may be deemed non-conforming and subject to the risk procedure of Article 79 of the AIA,[105] which could lead to an increase in the fines regime in Article 99 of the AIA.[106] Thus, logs must follow the AI system's legal footprint rather than its actual data centre footprint, regardless of the server's location, the duty to record, preserve, and surrender them remains fully enforceable.

4.2.3 Human Oversight

The human oversight standard is anchored to the product wherever it is operated. Even if the infrastructure and staff in charge of carrying out the oversight are located outside of the EEA, their legal weight is unaffected. As required by Article 14(4) of the AIA, the AI system must continue to provide explanation cues, real time status data, and reliable stop mechanism.[107]

The provider cannot use geography as a shield if foreign surveillance laws or network barriers make it more difficult for the operator to exercise those controls. Instead, it must implement organisational or technical safeguards, such as encrypted tunnels. Third country surveillance or discovery powers do not lessen the enforceability of AIA compliance objects, but they may make the access to them more difficult. However, no matter where in the world these duties are performed, they are legally non-negotiable because failure to produce intact documentation, logs, or oversight, exposes the provider to risk non-conformity findings under Article 79[108] and possible fines under Article 99.[109]

[103] Artificial intelligence Act, art 21 (2).
[104] Artificial intelligence Act, art 74 (12).
[105] Artificial intelligence Act, art 79.
[106] Artificial intelligence Act, art 99.
[107] Artificial intelligence Act, art 14(4).
[108] Artificial intelligence Act, art 79.
[109] Artificial intelligence Act, art 99.

5. ASSESSING OTHER POST-SCHREMS II DATA TRANSFER SAFEGUARDS

The *Schrems II* ruling upheld the importance of maintaining a high level of protection of personal data transferred from the EU to third countries. With its ruling, the CJEU addressed the problem of third country government access to data.[110] Instead of calling for the elimination of any potential risk, unlike the data protection authorities (DPAs), the CJEU left some doors open to allow businesses to continue transferring personal data outside the EU by making reference to the implementation of supplemented measures and the objective of attaining a sufficient degree of defence against the foreign governments access.[111]

As it happens, the regulatory winds are shifting again. There have already been two prominent legal motions, against the EU-US Data Privacy Framework (DPF), and the Adequacy Decisions. Max Schrems' NGO NOYB has publicly pledged that there will be a new case, *Schrems III.* NOYB is stating that the US surveillance legislation, FISA section 702 and EO 12333[112] now reinforced by the removal of members of the Privacy and Civil Liberties Oversight Board (PCLOB) in January 2025, consequently destroying the frameworks last independent oversight body, continue to violate Charter Articles 7, 8 and 47, and are therefore incompatible with EU fundamental rights standards.[113]

Meanwhile, French MP Philippe Latombe has filed Case T-553/23[114] before the CJEU to overturn the Adequacy Decisions. Interim measures in the case were rejected in 2023, however, the main action was admitted, and on April 3, 2025, the oral argument was held.[115]

5.1 Adequacy Decision and the EU-US Data Privacy Framework - Do They Still Hold?

If either, NOYB's or Latombe's, move is successful, the Data Privacy Framework (DPF) might fall apart as quickly as *Schrems II* destroyed the EU-US Privacy Shield, because when

---

[110] Christakis Theodore.'After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe', (European Law Blog, July 21, 2020), p. 2-3.
[111]Christakis 2024, note 32, p.17.
[112] *Ibid,* note 68.
[113] NOYB. 'US Cloud soon illegal? Trump punches first hole in EU-US Data Deal', (NOYB, 23 January 2025), Available online: https://noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal?utm_source=chatgpt.com (14.5.2025)
[114] T-553/23
[115] Standeford Dugie. 'EU Court Hears Arguments in Case Seeking Annulment of EU-U.S. Data Transfer Pact', (Privacy Daily, April 3 2025) Available online: https://privacy-daily.com/article/2025/04/03/eu-court-hears-arguments-in-case-seeking-annulment-of-euus-data-transfer-pact-2504030004?BC=bc_67ef88d7ced4d&utm_source=chatgpt.com (23.4.2025)

you take one away the other loses its effect. This is because the Adequacy Decision relies on two pillars, the enforcement of the DPF principles and the surveillance safeguards and redress mechanisms created by the EO 14086,[116] as mentioned in Chapter 3.1. Because the DPF and the Adequacy Decision are designed to work together, as explained in Chapter 1.3.2, policymakers and businesses must therefore keep an eye on the stability of both instruments when planning cross-border data transfers.

If either action succeeds, any transfers must be halted whenever the importer is stopped from upholding EU equivalent protections by foreign law, as discussed in Chapter 3.1, because the residual risk would still conflict with the Charter rights to privacy, data protection, and effective judicial redress.

5.2 Possible Schrems III Case

When the European Commission adopted the EU-US Data Privacy Framework (DPF) on 2023, NOYB branded it as "a copy of the failed Privacy Shield", and declared it was ready to take the decision back to the CJEU for a third round, because neither the FISA section 702 nor the EO 12333 had been reformed, as discussed in Chapter 3.1, and the redress bodies remained executive, not judicial.[117]

President Trump's January 2025 removal of the Privacy and Civil Liberties Oversight Board (PCLOB) members deprived it of the quorum it needs to function, transforming NOYB's earlier warning into an immediate threat to the DPF. The PCLOB's significance for the EU can be seen in the European Commission's Decision (EU) 2023/1795 regarding the Adequacy Decisions, because PCLOB is mentioned there 31 times as a proof that the US had an independent oversight body capable of monitoring intelligence agencies and enforcing the safeguards promised in the EO 14086.[118] By mentioning it so many times, they aimed to prove that the US safeguards really do match the EU's "essentially equivalent" protection standard. Therefore, once the PCLOB lost its quorum, the key proof was lost, weakening the whole Adequacy Decision, as well as the DPF, for they are linked together.

[116] Commission Implementing Decision EU 2023/1795, recitals 203 and 204.
[117] *Ibid,* note 68.
[118] Commission Implementing Decision EU 2023/1795

At the same time in January 2025, a 45-day review of the EO 14086, the second pillar of the deal, was initiated by a presidential order.[119] However, the EO 14086 has not been revoked. As a result, the EO 14086 continues to provide the proportionality restrictions and redress rules that support the Data Privacy Framework (DPF), although its future seems to be fragile. Therefore, NOYB is monitoring whether "the PCLOB is being killed for good", signalling that these events together will form the factual backbone of an eventual *Schrems III* case.[120]

The possibility that the DPF will survive *Schrems III* is unlikely, despite the revisions to US law and the European Commission's hard work on the issue. This means that particularly the call for a risk-based approach (instead of a "zero-risk" approach) to cross-border data transfers, would become even more crucial for transfers to the US. Not to mention the increased expenses and legal certainty, especially the EU based businesses would face, making these transfers instantly harder should these legal motions ever bear fruit.[121]

5.3 Risk-Based Approach - Proportionality test

Instead of using a "zero-risk" approach developed by the data protection authorities (DPAs), which demands the elimination of all risks to foreign unauthorised access, as mentioned in Chapter 1.3, the *Schrems II* ruling allows alternatively for a risk-based, proportionality test approach. The CJEU clarifies that supplementary measures do not offer a full guarantee that third parties will never be able to access data, rather it requires that they constitute "effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law".[122] Therefore, proportionality instead of perfection, should be the standard used for the "essentially equivalent" level of protection.[123]

If the possible *Schrems III* ruling were to annul the EU-US Data Privacy Framework (DPF), the Adequacy Decision that currently allows the frictionless cross-border transfers would be nullified. Every personal data flow to a US recipient, including those on the DPF list, would have to cease at that point or be "repapered" using a different GDPR Chapter V tool, most likely the standard contractual clauses (SCCs) together with the Transfer Impact Assessment (TIA). Businesses would rush to localise data, relocate to EU cloud regions, or harden their

[119] *Ibid,* note 113.
[120] *Ibid*
[121] Christakis 2024, note 32, p.13
[122] C-311/18, para 137.
[123] Breithbarth Paul. 'A Risk-Based Approach to International Data Transfers', (European Data Protection Law Review, Volume 7, issue 4, 2021, pp.539-549), p.548.

pipelines with privacy enhancing technologies. Exporters would then be immediately required to suspend or renegotiate the transfer, and regulators could impose fines on businesses that continued to use the outdated framework.

Because post-*Schrems II* data protection requirements allow for a risk-based proportionality test, transfers may take place if a set of organisational, contractual, and technical measures reduces the remaining risk to "essentially equivalent" level. The GDPR's accountability principle, Articles 5(2) and 24(1), requires controllers to maintain audit ready documentation proving the efficacy of their safeguards, which supervisors may request at any time. Meeting the proportionality test is part of that principle.[124]

The same is required under AIA, this comes back to what was discussed in Chapter 4, that evidence "travels with the system". The data streams produced by large scale AI training pipelines, such as training data, model output logs, and user feedback, always include bits of personal data. The full weight of Articles 11-14 and 18-22 of the AIA would still apply to high-risk AI providers that store documentation, logs, or oversight consoles in a third country cloud. Regulators must have the ability to access them as unaltered upon request, regardless their location.

In conclusion, if the DPF does fall, proportionality transforms from an option into a necessity. Exporters must demonstrate, through the GDPR accountability and AIA objects, that their SCC plus TIA based data transfer in conjunction with strong safeguards, such as encryption or pseudonymisation, maintain EU level "essentially equivalent" protection in real world conditions. Failure to do so means that the transfer must stop.

[124] GDPR, art 5(2) and 24(1).

6. AI INFRASTRUCTURE COMPLIANCE ON DATA LOCALISATION AND CLOUD ECOSYSTEMS

Operational and regulatory expectations regarding data sovereignty and security are growing as AI systems depend more and more on cloud based infrastructure. User control over data access and portability within the cloud ecosystem is greatly strengthened by the upcoming 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), which will become applicable in September 2025.[125]

The Data Act seeks to safeguard EU based businesses against unjust data sharing conditions imposed by powerful competitors and to advance fairness and competition in the EU cloud market.[126] Even though the Data Act focuses on non-personal data, it interacts with the GDPR. In cases when datasets include both personal and non-personal data, the GDPR's rules take precedence, providing comprehensive protection of personal data during cross-border transfers,[127] as discussed in Chapter 2.1.

Consequently, businesses handling this "mixed" data, which are most (if not all) of the AI providers, are being steered toward EU based cloud infrastructures that comply with the GDPR and, from September 2025 the Data Act's localisation and third country access rules,[128] and from 2 August 2027 they must also meet the AIA's high-risk obligations, the ones discussed in Chapters 4.2.1 - 4.2.3.[129] Together, these three regimes make storing and processing data inside the EU not only a legal necessity but an attractive competitive strategy, reinforcing the localisation pressures explored later in this chapter.

6.1 Data Localisation and Sovereign Clouds

Since *Schrems II*, a number of data protection authorities (DPAs) have adopted a "keep it in Europe" policy regarding sensitive datasets, occasionally even considering a foreign request

[125] 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), [2023] OJ L 2854
[126] European Commission. 'Data Act explained', (Last update 29 January 2025), Available Online: https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained (17.5.2025)
[127] Data Act, Recital 7.
[128] Data Act, art 50.
[129] Artificial Intelligence Act, art. 113(c).

for data held in the EU/EEA to be an unlawful disclosure.[130] This reflects the "zero-risk" approach that was introduced in Chapter 1.3. For instance, the French DPA, CNIL, mandates that "the risk of unlawful access to this data by the US authorities must be eliminated", even when data never leaves French territory.[131] Similar interpretation is evident in Germany, as the Baden-Württemberg Chamber of Public Procurement in its ruling stated that "an international transfer must also be presumed when personal data is placed on a platform accessible from a third country - regardless of whether access actually takes place". Continuing that "it is irrelevant whether the servers through which the data is made accessible are located in the EU".[132]

In addition, the European Union Agency for Cybersecurity has initiated the Cybersecurity Certification Regime for Cloud Services (EUCS). The draft version of the EUCS states that its aim would be to "harmonise the security of cloud services with EU regulations, international standards, best industrial practices, as well as with existing certifications in EU Member States".[133] At its highest assurance level, the EUCS requires full EU data localisation, EU headquartered providers, and limitations on non-EU shareholdings.[134]

As a result, localisation requirements have become a majour compliance hurdle for cross-border AI operations, standing alongside traditional cybersecurity and privacy obligations. However, as discussed in Chapter 5.3, the CJEU in *Schrems II* actually permits a more flexible, risk-based approach. According to this approach, data transfers may proceed if businesses implement and document safeguards that reduce residual access to a level considered "essentially equivalent" to EU standards.

To address these tightening localisation demands, businesses are increasingly integrating compliance into their technical structures by design. By storing highly sensitive data on regulatory approved clouds within its country of origin, cross-border exposure can be minimised from the beginning, the full elimination may prove difficult to implement as demonstrated earlier in the thesis.

---

[130] Christakis 2024, note 32, p.27.
[131] Christakis 2024, note 32, p. 28.
[132] Christakis 2024, note 32, p. 32.
[133] European Commission. 'EU Cloud Certification Scheme', (9.6.2021) Available online:https://ec.europa.eu/newsroom/cipr/items/713799/en (17.5.2025)
[134] Christakis 2024, note 32, p. 31-34.

These so-called "sovereign clouds" are specifically designed to guarantee that data is processed, stored, and managed solely within the jurisdiction of a specific country or region, shielding it from a third country's intervention or access.[135] In doing so, it eliminates the need for GDPR Chapter V mechanisms, such as standard contractual clauses (SCCs) plus supplementary measures under the GDPR, since the data never actually leaves the EU/EEA. Sovereign clouds therefore offer improved security, regulatory compliance, and control over data residency and are designed to comply with national or regional data protection laws. In contrast, public cloud services frequently span several jurisdictions and may expose data due to foreign surveillance legislation.[136]

Recognising this, the big hyperscalers have started to offer these sovereign cloud services that are used to store sensitive workloads. Examples include Amazon Web Services' "Digital Sovereignty", Microsoft's "European Data Boundary", and Google Cloud's "Digital Sovereignty", each featuring technical and contractual separation from non-EU access.[137] Many businesses are also adopting hybrid or multi-cloud strategies, using public global clouds for lower risk processes while keeping sensitive data in local, regulatory approved environments.[138]

Beyond infrastructure choices, innovative technical measures further embed compliance into AI system functionality. For instance, federated learning[139] and edge computing[140] allows models to be trained locally by transmitting only model updates, rather than raw data, therefore reducing the need for cross-border transfers and exposure to foreign surveillance.[141] Similarly, blockchain-based AI governance can create a tamper-proof, decentralised "memory" layer that documents every data handling event, providing regulators with

[135] Solanke Adedamola. 'Sovereign cloud implementation: Technical architectures for data residency and regulatory compliance', (International Journal of Science and Research Archive, April 2024), p. 2137-2138.
[136] *Ibid,* p. 2137-2138.
[137] Christakis 2024, note 32, p.27-28.
[138] Tewari Shishir, Chitnis Ashitosh. 'Ensuring Data Sovereignty in AI-Powered Multi- Cloud Enterprises', (IRE Journals, Volume 7, Issue 7, January 2024),p. 576.
[139] Definition by the European Data Protection Supervisor: "Federated learning is a relatively new way of developing machine-learning models where each federated device shares its local model parameters instead of sharing the whole dataset used to train it. The federated learning topology defines the way parameters are shared." Available online: https://www.edps.europa.eu/press-publications/publications/techsonar/federated-learning_en#:~:text=Federated%20learning%20is%20a%20relatively,the%20way%20parameters%20are%20shared. (16.5.2025)
[140] Definition by the European Commission: "edge computing data is processed in connected objects closer to the users. This allows for much faster operations and gives users more control over their data." Available online: http://digital-strategy.ec.europa.eu/en/library/cloud-and-edge-computing-different-way-using-it-brochure (16.5.2025)
[141] Tewari & Chitnis, note 138, p.576.

untampered proof of data locality throughout the data lifecycle, and supporting the launch of new, AI driven products and services.[142]

When taken as a whole, these strategies transform data localisation requirements from a mere legal obstacle into a central design principle and operational reality for AI systems.[143]

6.2 A Real Life Example - Microsoft EU Data Boundary

The Microsoft EU Data Boundary (EUDB) works as an example of one of the hyperscalers attempt to comply with the strict data transfer rules in the EU. The EUDB establishes a geographically enclosed environment where all system generated logs for Microsoft platforms, as well as customer provided content and professional services data, are processed and stored solely within the EU and European Free Trade Association region. The commitment went into effect recently, in February 2025, and is updated whenever new capabilities and services are added.[144]

In line with the traceability and logging requirements set out in the AIA, the EUDB incorporates pseudonymisation of operational logs in accordance with Article 4(5) of the GDPR. This reduces the risk that confidential information could be compromised by a third country's government surveillance powers.[145] Through the EUDB, Microsoft demonstrates how a hyperscale provider can reconcile the demands of modern cloud services with the EU's increasingly strict localisation and data protection regulations, offering a compliant route for cross-border AI and data transfer operations.

On paper, the EUDB offers a design that meets the GDPR's strict post-*Schrems II* cross-border data transfer requirements. As discussed in earlier chapters, these requirements have *de facto* led to demands for "data at rest localisation", meaning that keeping data in the EU/EEA is the simplest, and in some cases the only, way to ensure an "essentially equivalent" level of protection, and to avoid the complex measures that are otherwise necessary for legal cross-border transfers.

---

[142] European Investment Bank. 'Artificial intelligence, blockchain and the future of Europe', Available online: https://www.eib.org/en/publications/online/all/ai-blockchain-and-future-of-europe-report (16.5.2025)
[143] Tewari & Chitnis, note 138, p. 577-580.
[144] Microsoft. 'What is the EU data Boundary?', (26.02.2025) Available online: https://learn.microsoft.com/fi-fi/privacy/eudb/eu-data-boundary-learn#overview-of-the-eu-data-boundary (16.5.2025)
[145] *Ibid*

However, in practice the Microsoft EU Data Boundary (EUDB) cannot completely protect personal data from the US intelligence demands, even if the data never leaves the EU territory. Microsoft is still subject to US warrants and disclosure obligations requiring the transfer of data wherever it is held under FISA section 702, and also possibly EO 12333.[146] As highlighted in Chapter 5.3, France's data protection authority CNIL has made clear that any such request from US authorities, in relation to GDPR covered data processing, should be treated as an unauthorised disclosure under Article 48 of the GDPR. Therefore, Microsoft's EUDB does not deliver the statutory protection demanded by the EU, as a geographic separation alone does not exempt Microsoft from its legal obligations under the US surveillance laws. This also challenges the accountability principle in Article 5(2) of the GDPR and raises broader doubts about the sufficiency of purely technical or geographic controls in ensuring the lawfulness of cross-border data transfers.

In the future, the EUDB will most likely be further shaped by the new EU Data Act, which will impose more stringent regulations on, for example, unauthorised third country access. The EUDB's localisation measures will be strengthened by the Data Act's emphasis on openness, fairness in cloud contracts, and strong protection against third country data requests, as mentioned in Chapter 6, making it an even more compelling example of how providers need to comply with both the Data Act and the GDPR. Not to forget the impact of the, still in draft form, of Cybersecurity Certification Regime for Cloud Services (EUCS), introduced in Chapter 6.1. In practice, the EUDB could require more technical adjustments, more precise access controls, and more transparent policies about the management of data, regardless of its nature, inside the EU borders.

[146]Christakis 2024, note 32, p.28-29.

CONCLUSION

The thesis set out to determine to what extent the GDPR-AIA regime regulates cross-border data flows that fuel high-risk AI systems post-*Schrems II*. By following a hypothetical project from the birth of an AI system through model development, deployment, and post-market monitoring, the thesis found that the answer is: thoroughly, but on a risk-based proportionate basis.

The analysis demonstrates that the two regimes function as a single "safety chain" for the whole life cycle of the high-risk AI system. A GDPR data protection impact assessment (DPIA) must first justify why personal data needs to leave the EEA; a transfer impact assessment (TIA) assesses whether the destination country's surveillance laws would compromise a planned data transfer, and if gaps are found, specifies the supplementary measures needed, otherwise the transfer must stop; and an AIA fundamental rights impact assessment (FRIA) complements the previous assessments and includes the AI specific safeguards required for placing the system on the EU market. Each new dataset or AI model update creates an update and repeat loop that follows the AI system from the beginning to the market launch.

High-risk obligations under the AIA "travel with the system". Even when servers are located outside the EEA, documentation, log files, and human oversight consoles must be accessible in accordance with EU level confidentiality, integrity, and availability standards. Relocating them to a third country does not create a loophole, the enforceability of the AIA compliance is not diminished by third country surveillance powers. The Microsoft EU Data Boundary analysis illustrates the point: sovereign clouds can lower exposure, yet real world compliance still depends on provable encryption, EU only key custody and contractual vetoes that survive third country disclosure orders. Therefore, sovereign clouds mitigate but do not replace the legal and technical safeguards demanded by the GDPR-AIA regime.

Standard contractual clauses were preserved by the CJEU in its *Schrems II* ruling, but they can be used only with hard proof. Through TIAs and supplementary measures, exporters must demonstrate that any remaining surveillance exposure has been decreased to a level "essentially equivalent" to the EU level of protection. If bulk collecting regimes, such as FISA section 702, cannot be neutralised, the transfer must be suspended. The significance of

this case by case approach is only increased by the pending challenges to the Adequacy Decision and EU-US Data Privacy Framework.

Post-*Schrems II,* data protection authorities understandably aim for a "zero-risk" standard, in some cases demanding that all risks associated with foreign access be eliminated. However, the thesis demonstrates that complete elimination is both legally and technically unattainable, especially as CJEU through *Schrems II* permits a risk-based proportionality approach. If documented layers of organisational, contractual and technical measures cut the remaining risk to a minimum, the data transfer is acceptable.

Taken together, the GDPR-AIA regime governs the whole outbound pipeline. It obliges EU businesses to document every safeguard, update the DPIA-TIA-FRIA chain whenever circumstances change, and suspend any flow that cannot satisfy the "essentially equivalent" level of EU protection. Geographical factors may result in additional expenses and delays, but they never weaken EU fundamental right requirements. By embracing proportionality over perfection and integrating compliance into AI system design from the beginning, European businesses can take part in global, data driven AI innovation, without breaching the EU fundamental rights lines.

BIBLIOGRAPHY

Used Normative Material

1. Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, [2023] OJ L 231
2. Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7
3. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1
4. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, [2021] OJ L 199
5. Commission Nationale Informatique & Libertés. 'Practical Guide Transfer Impact Assessment', (Final version, January 2025)
6. Communication from the Commission to the European Parliament and the Council Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM/2019/250 final
7. Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation
8. EDPB. ‘Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models’ (Adopted on 17 December 2024)
9. EDPB. ‘Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data’, (Version 2.0, Adopted on 18 June 2021)

10. EDPB. ‘Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework’, (Version 1.1, Adopted on 4 November 2024)
11. H.R.7888 - Reforming Intelligence and Securing America Act, 118th Congress (2023-2024)
12. 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), [2016] OJ L 119
13. 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), [2023] OJ L 2854
14. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), [2024] OJ L 1689

Used Case-law

1. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, C-311/18.
2. Patrick Breyer v Bundesrepublik Deutschland, C-582/14
3. T-553/23 Latombe v Commission [2023] OJ C/2023/348

Used Literature

1. Breithbarth Paul. ‘A Risk-Based Approach to International Data Transfers’, (European Data Protection Law Review, Volume 7, issue 4, 2021, pp.539-549)
2. Christakis Theodore. 'The Zero Risk Fallacy: International Data Transfers, Foreign Governments’ Access to Data and the Need for a Risk-Based Approach', (Centre for Information Policy Leadership, Cross-Border Data Forum, February 2024)

3. Christakis Theodore.‘After Schrems II :Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe’, (European Law Blog, July 21, 2020)
4. Connolly Matthew. ‘WILL THE EU-US DATA PRIVACY FRAMEWORK
5. SURVIVE SCHREMS III?’, (Trinity College Law Review, Volume 27, 2024, pp. 87-124.)
6. Fahey Elaine. ‘Strategic Litigation and EU Law on Cross-Border Data Transfers: On the Place of EU Law in the Work of Schrems and NOYB’, (Nordic Journal of European Law, Volume 7, Issue 4, 2024)
7. Giovanni Tricco. 'The New Transatlantic Data Agreement Placed in Context: Decoding the Schrems Saga within the Digital Economy', (Journal of Law, Market & Innovation, Vol 3 - Issue 1/2014)
8. Gulbakyt Bolatbekkyzy. ‘Legal issues of cross-border data transfer in the era of digital government’, (Journal of Digital Technologies and Law, 2024)
9. Kokoulina Olga. 'Challenges in Digital Compliance: Risk Assessment and Fundamental Rights under the GDPR and the EU AI Act', (Paper presented at Processes, Laws and Compliance workshop at the 6th International Conference on Process Mining, University of Copenhagen, 2024)
10. Kseng San. 'International Collaboration in AI Research and Development', (International IT Journal of Research, Volume 2, Issue 1, Jan-March 2024)
11. Pandit Harshvardhan J., Rintamäki Tytti. ‘Towards An Automated AI Act FRIA Tool That Can Reuse GDPR’s DPIA’, (Presented at CLAIRvoyant (ConventicLE on Artificial Intelligence Regulation) Workshop 2024)
12. Rintamäki Tytti, Golpayegani Delarm, Lewis Dave, Celeste Edoardo, Pandit Harshvardhan J.. 'High-Risk Categorisations in GDPR vs AI Act: Overlaps and Implications', (ADAPT SFI Research Centre at Dublin City University and Trinity College Dublin,Volume 11, 2023)
13. Solanke Adedamola. ‘Sovereign cloud implementation: Technical architectures for data residency and regulatory compliance’, (International Journal of Science and Research Archive, April 2024)
14. Tewari Shishir, Chitnis Ashitosh. ‘Ensuring Data Sovereignty in AI-Powered Multi-Cloud Enterprises’, (IRE Journals, Volume 7, Issue 7, January 2024)

15. Tricco Giovanni.‘The New Transatlantic Data Agreement Placed in Context: Decoding the Schrems Saga With the Digital Economy’, (Journal of Law, Market & Innovation, Volume 3, Issue 1/2024)
16. Zac Amit, Wey Pablo, Bechtold Stefan, Rodriguez David, Del Alamo Jose M. ‘The Court Speaks, But Who Listens? Automated Compliance Review of the GDPR’, (Center for Law & Economics Working Paper Series, 01/2024, updated version March 2024)

Used Online Sources:

1. European Commission. ‘Data Act explained’, (Last update 29 January 2025), Available Online: https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained (17.5.2025)
2. European Commission. ‘EU Cloud Certification Scheme’, (9.6.2021) Available online:https://ec.europa.eu/newsroom/cipr/items/713799/en (17.5.2025)
3. European Commission, ‘Europe’s Potential in Edge Computing: Supporting Industrial Innovation Through Large Scale Pilots’ (30 November 2023), Available online: Available online: http://digital-strategy.ec.europa.eu/en/library/cloud-and-edge-computing-different-way-using-it-brochure (16.5.2025)
4. European Data protection Supervisor. ‘Federated Learning’ Available online: Available online: https://www.edps.europa.eu/press-publications/publications/techsonar/federated-learning_en#:~:text=Federated%20learning%20is%20a%20relatively,the%20way%20parameters%20are%20shared. (16.5.2025)
5. European Investment Bank. ‘Artificial intelligence, blockchain and the future of Europe’, Available online: https://www.eib.org/en/publications/online/all/ai-blockchain-and-future-of-europe-report (16.5.2025)
6. Microsoft. ‘What is the EU data Boundary?’, (26.02.2025) Available online: https://learn.microsoft.com/fi-fi/privacy/eudb/eu-data-boundary-learn#overview-of-the-eu-data-boundary (16.5.2025)
7. NOYB. 'European Commission gives EU-US data transfers third round at CJEU', (NOYB, 10 July 2023) Available online:

https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu?utm_source=chatgpt.com (23.4.2025)

8. NOYB. ‘US Cloud soon illegal? Trump punches first hole in EU-US Data Deal’, (NOYB, 23 January 2025), Available online: https://noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal?utm_source=chatgpt.com (14.5.2025)
9. Standeford Dugie. 'EU Court Hears Arguments in Case Seeking Annulment of EU-U.S. Data Transfer Pact', (Privacy Daily, April 3 2025) Available online: https://privacy-daily.com/article/2025/04/03/eu-court-hears-arguments-in-case-seeking-annulment-of-euus-data-transfer-pact-2504030004?BC=bc_67ef88d7ced4d&utm_source=chatgpt.com (23.4.2025)
10. Squark. ‘What’s an “AI Pipeline”, (Squark, 20 November 2022), Available online: https://squarkai.com/whats-an-ai-pipeline/#:~:text=An%20AI%20Pipeline%20is%20an,parameters%2C%20and%20other%20prediction%20outputs (17.5.2025)