MASTER THESIS | MASTER'S THESIS

Titel | Title

Managing International Data Flows: Strategies and Challenges of GDPR Compliance in International Corporations

verfasst von | submitted by

mgr Agnieszka Weronika Wudarczyk

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 999 082
Universitätslehrgang lt. Studienblatt | Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht (LL.M.)
Betreut von | Supervisor:	ao. Univ.-Prof. Mag. Dr. Siegfried Fina

Abstract

(English)

This thesis focuses on analysing the approaches taken and the issues arising when international corporations apply measures to control the transfer of personal data for GDPR compliance. The study uses a legal research approach whereby the legal framework governing data protection in multiple jurisdictions is analysed through legal cases, compliance reports, and legislation to establish how international corporations work under the data protection regimes. The findings of this research indicate that GDPR compliance is best achieved through technical solutions such as data encryption and utilization of data discovery tools implemented together with organisational solutions such as appointment of data protection officers and conduction of intra-organization training programmes and reliance on legal solutions such as standard contractual clauses and binding corporate rules. Some of the current issues highlighted include the lack of harmonised legal requirements across different jurisdictions, lack of uniformity in the enforcement of the existing laws, practical matters in compliance with the laws across the operations, and the clash between the GDPR and other laws binding outside of European Union. Special emphasis is placed on the consequences of the recent judgement in the Schrems II case, which has led to a complete reconsideration of the transfer of data across borders. The research findings show that this decision has implications beyond EU-US transfers, including data transfers to all other third countries and necessitating higher standard reviews of third-country laws. This thesis serves a valuable purpose in the existing literature on international data protection by offering practical recommendations on compliance measures, highlighting significant current issues, and evaluating the effects of primary legislation. It provides advice for international business and outlines further research directions in the development of this emerging area.

Keywords: GDPR compliance, international data flows, data protection, Schrems II, cross-jurisdictional challenges

Abstract
(Deutsch)

Diese Arbeit konzentriert sich auf die Analyse der Ansätze und Probleme, die sich ergeben, wenn internationale Unternehmen Maßnahmen zur Kontrolle der Übermittlung personenbezogener Daten zur Einhaltung der DSGVO ergreifen. Die Studie verwendet einen juristischen Forschungsansatz, bei dem der rechtliche Rahmen für den Datenschutz in mehreren Rechtsordnungen anhand von Rechtsfällen, Compliance-Berichten und Gesetzgebungen analysiert wird, um festzustellen, wie internationale Unternehmen unter den Datenschutzregelungen arbeiten. Die Ergebnisse dieser Untersuchung zeigen, dass die Einhaltung der DSGVO am besten durch technische Lösungen wie Datenverschlüsselung und den Einsatz von Datenermittlungstools in Verbindung mit organisatorischen Lösungen wie der Ernennung von Datenschutzbeauftragten und der Durchführung von organisationsinternen Schulungsprogrammen sowie durch rechtliche Lösungen wie Standardvertragsklauseln und verbindliche Unternehmensregeln erreicht werden kann. Zu den derzeitigen Problemen zählen unter anderem das Fehlen harmonisierter gesetzlicher Anforderungen in verschiedenen Rechtsordnungen, die uneinheitliche Durchsetzung bestehender Gesetze, praktische Fragen bei der Einhaltung der Gesetze im gesamten Betriebsablauf und der Konflikt zwischen der DSGVO und anderen außerhalb der Europäischen Union geltenden Gesetzen. Besonderes Augenmerk wird auf die Folgen des jüngsten Urteils im Fall Schrems II gelegt, das zu einer vollständigen Überprüfung des grenzüberschreitenden Datentransfers geführt hat. Die Forschungsergebnisse zeigen, dass diese Entscheidung Auswirkungen über den Datenverkehr zwischen der EU und den USA hinaus hat, einschließlich des Datenverkehrs in alle anderen Drittländer, und eine strengere Überprüfung der Gesetze von Drittländern erforderlich macht. Diese Arbeit leistet einen wertvollen Beitrag zur bestehenden Literatur zum internationalen Datenschutz, indem sie praktische Empfehlungen zu Compliance-Maßnahmen gibt, wichtige aktuelle Probleme aufzeigt und die Auswirkungen der Primärgesetzgebung bewertet. Sie bietet Ratschläge für internationale Unternehmen und skizziert weitere Forschungsrichtungen für die Entwicklung dieses aufstrebenden Bereichs.

Stichworte: DSGVO-Konformität, internationale Datenströme, Datenschutz, Schrems II, grenzüberschreitende Herausforderungen

Table of Contents

Chapter 1: Introduction

1.1 Background on GDPR and international data flows

International corporations (hereinafter referred to also as: globally operating companies) understood as enterprises producing goods or delivering services in more than one country[1] rely substantially on personal data transfers in their day-to-day operations[2]. Thus, in today's rapidly evolving global economy international personal data transfers are one of the underpinnings for globally operating companies.

Businesses have communication between their branches all over the world for the corporate goals of the business.[3] This demand for the extreme availability of information often contrasts with the new tendencies concerning the protection of personal data.[4] The General Data Protection Regulation (GDPR) has now become the foundation of data protection across the world. The GDPR, implemented on 25 May 2018, changed the processing and transfer of personal data within and outside the member states of the European Union.[5]

Under Article 3, the GDPR's reach extends beyond EU borders to include any organisation that handles EU residents' personal data. This means that businesses worldwide need to follow these rules anytime they process information pertaining to EU residents, irrespective of the location of the business.[6] This broad scope has led international organisations to rethink how they approach data completely.[7] The problems with international data transfers that the GDPR raises are multiple and multifaceted. Despite the fact that the regulation is to promote the availability and cross-border data flow within the Internal Market of the EU due to the economic

---

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Multinational_enterprise_(MNE) accessed 6 April 2025, 17:39

[2] Zlatko Delev, Managing International Data Transfers under GDPR and Beyond https://gdprlocal.com/managing-international-data-transfers-under-gdpr-and beyond/#:~:text=We%20live%20in%20a%20world,just%20interested%20in%20the%20topic. accessed 6 April 2025, 17:56

[3] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013) 2-3. https://doi.org/10.1093/acprof:oso/9780199674619.001.0001 accessed 20 October 2024, 11:11

[4] Lokke Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (Oxford University Press 2012) 5-7. https://doi.org/10.1093/acprof:oso/9780199662913.001.0001 accessed 20 October 2024, 11:12

[5] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 2. http://dx.doi.org/10.1007/978-3-319-57959-7 accessed 20 October 2024, 11:16

[6] Article 3 GDPR. https://gdpr-info.eu/art-3-gdpr/ accessed 20 October 2024, 11:17

[7] Maja Brkan and Evangelia Psychogiopoulou (eds), *EU Data Protection Law and Policy* (Edward Elgar Publishing 2021) 205. http://www8.austlii.edu.au/cgi-bin/viewdoc/au/journals/ELECD/2017/672.html accessed 20 October 2024, 11:17

significance,[8] it also imposes strict requirements on transferring personal data to non-EU countries and international organisations, as detailed in Chapter V.[9] This has created a challenging legal environment where international businesses must balance maintaining data flow while ensuring robust personal data protection.[10]

1.2 Significance of the study

The importance of this research is based on the identified research gaps in the literature on GDPR compliance and cross-border data transfers. Although there has been an increase in the number of publications concerning the GDPR and its implications for organisations, there are still relatively few studies available that focus on the practical approaches to GDPR compliance for international business organisations.[11] The issues related to compliance maintenance across the jurisdictions have not been studied to the extent, especially regarding the differences in legal frameworks and enforcement.[12] This gap in knowledge is particularly pronounced when considering the complexities faced by multinational corporations operating across diverse regulatory landscapes.[13]

Furthermore, the landmark judgment of the Court of Justice of the European Union (CJEU) in the case of *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (commonly known as *Schrems II*) has added another layer of complexity to the international data transfer landscape.[14] Although *Schrems II* has been discussed widely in academia and among professionals, there is still little research that addresses the consequences of this particular judgement, not only for the EU-US transfer of personal data but for the transfer of

---

[8] Recital 13 GDPR. https://gdpr-info.eu/recitals/no-13/ accessed 20 October 2024, 11:19
[9] Chapter V GDPR. https://gdpr-info.eu/chapter-5/ accessed 20 October 2024, 11:19
[10] Lokke Moerel, 'GDPR conundrums: The data transfer conundrum' (2020) 169 Computer Law & Security Review 1. https://assets.contentstack.io/v3/assets/blt5775cc69c999c255/blt4acf7754cc1e1db6/160719gdprconundrumsdpo.pdf accessed 20 October 2024, 11:20
[11] Gonçalo Almeida Teixeira, Miguel Mira da Silva and Ruben Pereira, 'The Critical Success Factors of GDPR Implementation: A Systematic Literature Review' (2019) 21(4) *Digital Policy, Regulation and Governance* 402. https://doi.org/10.1108/DPRG-01-2019-0007 accessed 20 October 2024, 11:22
[12] Maja Brkan, 'The Court of Justice of the EU, Privacy and Data Protection: Judge-made Law as a Leitmotif in Fundamental Rights Protection' in Maja Brkan and Evangelia Psychogiopoulou (eds), *Courts, Privacy and Data Protection in the Digital Environment* (Edward Elgar Publishing 2017). https://doi.org/10.4337/9781784718718.00009 accessed 20 October 2024, 11:23
[13] W. Gregory Voss, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29(3) Washington International Law Journal 485. https://digitalcommons.law.uw.edu/wilj/vol29/iss3/7/ accessed 20 October 2024, 11:25
[14] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* [2020] ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311 accessed 20 October 2024, 11:30

such data from the EU to the rest of the world.[15] This research will fill these gaps by presenting a systematic analysis of the approaches, issues, and legal consequences of GDPR compliance concerning international data transfers. In this way, it aims to provide significant research findings to the theoretical and empirical literature and the practise of international data protection.[16]

1.3 Overview of GDPR's impact on international corporations

The GDPR has had a profound impact on international corporations, compelling them to reassess and often overhaul their data management practices fundamentally.[17] The regulation's broad definition of personal data, coupled with its expansive territorial scope, means that virtually all multinational entities dealing with EU residents' data fall under its purview.[18] One of the most significant impacts has been on international data transfers. The GDPR's strict requirements for transferring personal data outside the EU, as outlined in Articles 44-50, have necessitated a careful review of data flows and the implementation of appropriate safeguards.[19] This has been mainly tested on corporations with operations across the world because they have to make sure they are legal in all the locations they operate in.[20]

The introduction of the concept of 'data protection by design and by default' in Article 25 of the GDPR has also necessitated changes in how international corporations approach product and service development.[21] This principle requires entities to integrate data protection considerations into their business processes from the outset rather than as an afterthought.[22] The enforcement measures provided for in the GDPR, such as the new substantial fines of up to 4% of the worldwide turnover, have taken data protection to new board-level logic for

---

[15] Christopher Kuner, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (2020) 23 European Law Review 1. http://www.kuner.com/my-blog-entries.html accessed 20 October 2024, 11:30

[16] Gonçalo Almeida Teixeira, Miguel Mira da Silva and Ruben Pereira, 'The Critical Success Factors of GDPR Implementation: A Systematic Literature Review' (2019) 21(4) *Digital Policy, Regulation and Governance* 402 https://doi.org/10.1108/DPRG-01-2019-0007 accessed 20 October 2024, 11:30

[17] Eline Chivot and Daniel Castro, 'What the Evidence Shows About the Impact of the GDPR After One Year' (Center for Data Innovation, 17 June 2019) https://datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/ accessed 20 October 2024, 11:30

[18] Article 4(1) GDPR. https://gdpr-info.eu/art-4-gdpr/ accessed 20 October 2024, 11:33

[19] Articles 44-50 GDPR. https://gdpr-info.eu/chapter-5/ accessed 20 October 2024, 11:35

[20] W Kuan Hon and Christopher Millard, 'Banking in the Cloud: Part 3 – Contractual Issues' (2018) 34 Computer Law & Security Review 595 https://doi.org/10.1016/j.clsr.2017.11.007 accessed 20 October 2024, 11:35

[21] Article 25 GDPR. https://gdpr-info.eu/art-25-gdpr/ accessed 20 October 2024, 11:36

[22] Aurelia Tamò-Larrieux, *Designing for Privacy and its Legal Framework* (Springer 2018) 8-10. https://doi.org/10.1007/978-3-319-98624-1 accessed 20 October 2024, 11:37

numerous global businesses.[23] This has led to increased investment in data protection measures and a growing recognition of data protection as a key business risk.[24]

The *Schrems II* decision has again turned the international corporations' world upside down. This means that the decision to invalidate the EU-US Privacy Shield and to add new requirements to the use of Standard Contractual Clauses (SCCs) have required a holistic rethink of international data transfers.[25] This has particularly affected corporations relying on transatlantic data flows, but its implications extend to data transfers to all third countries.[26]

1.4 Aim of the thesis

The primary aim of this thesis is to conduct a comprehensive analysis of how international corporations manage the flow of personal data to ensure compliance with GDPR regulations, with a particular focus on entities that have establishments both inside and outside the EU. This research is driven by the pressing need to understand the practical strategies employed by these corporations in addressing the legal challenges posed by international data flows, as well as to identify the key obstacles they face in maintaining compliance across different jurisdictions.[27]

To this end, this study will address the following research questions:

1. How do internationally operating corporations manage the flow of personal data to ensure compliance with GDPR regulations?
2. What are the key challenges faced by internationally operating corporations in maintaining GDPR compliance across different jurisdictions?

---

[23] Article 83 GDPR. https://gdpr-info.eu/art-83-gdpr/ accessed 20 October 2024, 11:39
[24] DLA Piper, 'GDPR Data Breach Survey 2022' (DLA Piper, January 2022) https://www.dlapiper.com/en/insights/publications/2022/01/dla-piper-gdpr-fines-and-data-breach-survey-2022/ accessed 20 October 2024, 11:40
[25] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (10 November 2020). https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en accessed 20 October 2024, 11:42
[26] Svetlana Yakovleva and Joris Van Hoboken, 'The Algorithmic Learning Deficit: Artificial Intelligence, Data Protection, and Trade' [2020] SSRN Electronic Journal https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3668434 accessed 20 October 2024, 11:43
[27] Bart Custers, Alan M. Sears, Francien Dechesne, Ilina Georgieva, Tommaso Tani, and Simone van der Hof, *EU Personal Data Protection in Policy and Practice* (T.M.C. Asser Press 2019) 25-30. https://content.e-bookshelf.de/media/reading/L-12309078-f1670d5329.pdf accessed 20 October 2024, 11:43

3. What are the implications of the *Schrems II* decision on the international data flow practices of internationally operating corporations, not only for EU-US transfers but also for data flows from the EU to the rest of the world?

The following hypotheses underpin these questions:

1. International corporations adopt a range of strategies to manage GDPR compliance, including technical, organisational, and legal measures.
2. Key challenges include varying legal standards, enforcement practices across jurisdictions, and operational complexities.
3. The *Schrems II* decision has significant implications, requiring corporations to reassess and adjust their data transfer mechanisms, with potential impacts extending beyond EU-US transfers to affect data flows to all third countries.

By addressing these questions and testing these hypotheses, this thesis aims to contribute to a more nuanced understanding of the practical realities of GDPR compliance in the context of international data flows.[28]

1.5 Structure of the thesis

The structure of this thesis is designed to provide a comprehensive exploration of the research questions and hypotheses outlined above. It is organised as follows:

Chapter 2 will provide a comprehensive literature review, exploring existing research on GDPR compliance strategies, theoretical frameworks for data protection in international contexts, and key concepts related to international data flows. This chapter will also identify gaps in the current literature, further justifying the need for this research.[29] Chapter 3 will outline the research methodology in detail, including the rationale behind the chosen approach and the methods of data collection and analysis. This chapter will explain how legal documents,

[28] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 65-70. https://books.google.com/books?hl=en&lr=&id=jCXYCgAAQBAJ&oi=fnd&pg=PP1&dq=Orla+Lynskey,+The+Foundations+of+EU+Data+Protection+Law+(Oxford+University+Press+2015)+65-70.+&ots=iYe095FvBh&sig=x7_TWFDUP0w7zYSUkDzDcH2gow4 accessed 20 October 2024, 11:43

[29] Lee A. Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014) 12-15. http://dx.doi.org/10.1093/acprof:oso/9780199675555.001.0001 accessed 20 October 2024, 11:49

compliance reports, case law, academic literature, and industry reports will be analysed to address the research questions.[30]

Chapter 4 will delve into the strategies adopted by international corporations to manage GDPR compliance in their data flows. This will include an examination of technical measures such as encryption and pseudonymisation, organisational measures like the appointment of Data Protection Officers, and legal measures including the use of Standard Contractual Clauses and Binding Corporate Rules.[31] Chapter 5 will discuss the difficulties experienced by international operational corporations in compliance with GDPR across borders. This will take form in the comparison of legal standards that differ and enforcement discrepancies, as well as the running of operations that come with virtual facility management across different regulatory frameworks.[32]

Chapter 6 will look at the impact of the Schrems II decision on the flow of data internationally with a deeper explanation of the issues involved. This chapter will not only evaluate the effects of the CJEU decision on the EU-US data transfers but will also discuss other potential consequences for data transfers from the EU to other third countries in accordance with the supervisor's recommendations.[33] Chapter 7 will present the findings of the research, synthesising the insights gained from the analysis of compliance strategies, challenges, and the *Schrems II* implications. This chapter will also concern itself with a discussion of the implications of these findings in light of the research questions and hypotheses formulated at the beginning of this study.[34] Finally, Chapter 8 will provide the conclusion of the thesis, present the main conclusions drawn, discuss the impact of the results on international

[30] *Ibid.*
[31] Robert K. Yin, *Case Study Research and Applications: Design and Methods* (6th edn, SAGE Publications 2017) 25-66. https://www.google.com/books/edition/Case_Study_Research_and_Applications/6DwmDwAAQBAJ accessed 20 October 2024, 11:50
[32] Kristina Irion, 'Panta Rhei: A European Perspective on Ensuring a High-Level of Protection of Digital Human Rights in a World in Which Everything Flows' (30 June 2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3638864 accessed 20 October 2024, 11:51
[33] Christopher Kuner, 'The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation' (2020) European Law Blog. http://www.kuner.com/my-blog-entries.html accessed 20 October 2024, 11:55
[34] Liane Colonna, 'Data Mining and EU Data Protection Law: Challenges for Big Data Analysis in the GDPR Era' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds), *New Technology, Big Data and the Law* (Springer 2017) 115-142. DOI: 10.1007/978-981-10-5038-1_6 https://link.springer.com/book/10.1007/978-981-10-5038-1 accessed 20 October 2024, 11:55

companies and tendencies in the protection of data, and reveal the possibilities for further research.[35]

By maintaining a dominant emphasis on the data flow within internationally operating corporations throughout this thesis, we aim to provide valuable insights into the legal challenges and practical realities of GDPR compliance in a global context. This research aspires to contribute meaningfully to the ongoing discourse on international data protection, offering both theoretical understanding and practical guidance for corporations navigating the complex landscape of global data flows in the age of the GDPR.[36]

Chapter 2: Literature Overview and Theoretical Framework

2.1 Introduction

The General Data Protection Regulation (GDPR) has significantly altered the landscape of data protection and privacy, particularly in international data flows. This chapter aims to provide a comprehensive overview of existing research on GDPR compliance strategies, theoretical frameworks for data protection in international contexts, and key concepts related to international data flows. Additionally, it will identify and discuss the research gaps that this thesis aims to address.

2.2 Existing Research on GDPR Compliance Strategies

Since the implementation of the *General Data Protection Regulation* (GDPR) in May 2018, a growing body of literature has emerged focusing on compliance strategies for organisations.[37] These studies can be broadly categorised into technical, organisational, and legal approaches to GDPR compliance. Each of these approaches provides a specific view and solutions for managing the challenging aspects of the GDPR, especially regarding cross-border data transfers.

---

[35] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020) 131-166. https://doi.org/10.1093/oso/9780190088583.001.0001 accessed 20 October 2024, 11:55

[36] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 1-3. https://link.springer.com/book/10.1007/978-3-319-57959-7 accessed 20 October 2024, 11:56

[37] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 1-3. http://dx.doi.org/10.1007/978-3-319-57959-7 accessed 20 October 2024, 11:57

2.2.1 Technical Approaches

Technical solutions to GDPR compliance mainly centre on the application of different technologies in order to protect data. These are grounded on Article 25 of GDPR- Data Protection by Design and by Default principle.[38] This principle demands an organisation adopt suitable technical and organisational measures to comply with data protection principles within processing operations. Gürses et al. provide a comprehensive overview of privacy-enhancing technologies (PETs) that can be employed to enhance data protection and are directly applicable to achieving GDPR compliance.[39] They discuss various techniques, such as data minimisation, pseudonymisation, and encryption, which are explicitly mentioned in the GDPR as appropriate technical measures.[40] Their research also tends to stress the necessity of incorporating these technologies into the data processing life cycle to maintain compliance.

Encryption, in general, has been discussed in detail as one of the most important means of safeguarding personal data transfers across borders. As highlighted by Monika Zalnieriute, end-to-end encryption can significantly reduce the risk of unauthorised access to personal data during cross-border transfers.[41] However, the effectiveness of encryption in ensuring GDPR compliance has been debated, particularly in light of the *Schrems II* decision, which emphasised the need for supplementary measures beyond encryption.[42] The *Schrems II* decision has led to increased scrutiny of technical measures for international data transfers. Kuner argues that while encryption and other technical measures are important, they may not be sufficient on their own to meet the GDPR's requirements for international transfers, particularly when transferring data to countries without adequate data protection laws.[43] This

[38] 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 L119/1, art 25. https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed 20 October 2024, 11:57

[39] Seda Gürses, Carmela Troncoso and Claudia Diaz, 'Engineering Privacy by Design Reloaded' (Amsterdam Privacy Conference, October 2015) https://software.imdea.org/~carmela.troncoso/papers/Gurses-APC15.pdf accessed 20 October 2024, 11:58

[40] GDPR, art 32. https://gdpr-info.eu/art-32-gdpr/ accessed 20 October 2024, 11:58

[41] Monika Zalnieriute, 'Data Transfers After Schrems II: The EU-US Disagreements Over Data Privacy and National Security' (2022) 55 *Vand J Transnat'l L* 1 https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/vantl55&section=4 accessed 20 October 2024, 11:59

[42] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020] ECLI:EU:C:2020:559. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62018CN0311:EN:HTML accessed 20 October 2024, 12:00

[43] Christopher Kuner, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (2020) European Law Blog. http://www.kuner.com/my-blog-entries.html accessed 20 October 2024, 12:00

has created a lot of interest in other measures that can be adopted to complement encryption so as to improve the protection of data being transferred across borders.

Another technical approach that has drawn light is Privacy by Design (PbD), a notion put in Article 25 of the GDPR.[44] Cavoukian and Castro argue that implementing PbD principles can help organisations achieve GDPR compliance more effectively by integrating privacy considerations into the design and architecture of IT systems and business practices.[45] They introduce seven key principles for the PbD framework, which is the approach to implementing PbD: proactive, not reactive; privacy as the default; design for privacy; at least proportional to risk; technology neutral; consider human factors; and privacy enhanced by default. Blockchain and AI have been considered potential solutions for improving GDPR compliance.

In their work, Zheng et al. describe how blockchain technology can be utilised to improve data protection and data privacy acceding to the GDPR.[46] They propose a blockchain-based personal data management system that gives individuals greater control over their data, aligning with the GDPR's principle of data subject rights. The use of these technologies also presents new challenges for GDPR compliance. As pointed out by Finck, while blockchain technology offers potential benefits for data protection, its immutable nature can conflict with the GDPR's right to erasure (Article 17).[47] Similarly, the use of AI in data processing raises questions about algorithmic transparency and the right to explanation, as discussed by Wachter et al.[48]

2.2.2 Organisational Approaches

The organisational perspective of GDPR compliance is centred on the administration of a framework for managing compliance with the regulation. These approaches acknowledge that

---

[44] GDPR, art 25. https://gdpr-info.eu/art-25-gdpr/ accessed 20 October 2024, 12:01

[45] Ann Cavoukian and Daniel Castro, 'Big Data and Innovation, Setting the Record Straight: De-identification Does Work' (2014) Information Technology and Innovation Foundation. https://www2.itif.org/2014-big-data-deidentification.pdf accessed 20 October 2024, 12:03

[46] Zibin Zheng and others, 'An Overview on Smart Contracts: Challenges, Advances and Platforms' (2020) 105 Future Generation Computer Systems 475. https://doi.org/10.1016/j.future.2019.12.019 accessed 20 October 2024, 12:04

[47] Michèle Finck, 'Blockchains and Data Protection in the European Union' (2018) 4 European Data Protection Law Review 17. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/edpl4&section=8 accessed 20 October 2024, 12:05

[48] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76. https://academic.oup.com/idpl/article-pdf/doi/10.1093/idpl/ipx005/17932196/ipx005.pdf accessed 20 October 2024, 12:07

GDPR is less of a technical problem than it is one of organisational culture and practises. One of them is a requirement to appoint the so-called Data Protection Officer (DPO) provided by Article 37 of the GDPR for certain categories of organisations.[49] Lachaud provides an in-depth analysis of the role of DPOs in ensuring GDPR compliance. He postulates that DPOs serve as compliance points as well as the point of recourse on behalf of data subjects.

According to Tikkinen-Piri et al., the elements of the proposed approach emphasise the need to develop a data protection-oriented organisational culture.[50] The authors opine that GDPR compliance entails a change of culture in organisations where data protection practise becomes a cultural issue rather than regulatory. They specified some organisational enabler improvements for GDPR readiness: organisations must set up data governance frameworks, employee awareness and training, and data breach management processes. Another key area of compliance that has been given much importance throughout the organisations and brought out clearly in Article 5(2) of the GDPR is accountability.[51]

Felzmann et al. discuss how organisations may establish accountability measures for the GDPR and identify that documentation of processing activities and data protection impact assessments are ways of proving that GDPR has been adhered to.[52] They argue that accountability goes beyond mere compliance, requiring organisations to take a proactive approach to data protection. The implementation of data protection impact assessments (DPIAs), as required by Article 35 of the GDPR, has been identified as a key organisational strategy for ensuring compliance.[53] Bieker et al. propose a methodology for conducting DPIAs that integrates legal, technical, and organisational perspectives.[54] They claimed DPIAs should be regarded not only as a compliance instrument but as a chance for organisations to evaluate and enhance their data processing activities critically.

---

[49] GDPR, art 37. https://gdpr-info.eu/art-37-gdpr/ accessed 20 October 2024, 12:08
[50] Christina Tikkinen-Piri, Anna Rohunen and Jouni Markkula, 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 Computer Law & Security Review 134. https://doi.org/10.1016/j.clsr.2017.05.015 accessed 20 October 2024, 12:08
[51] GDPR, art 5(2). https://gdpr-info.eu/art-5-gdpr/ accessed 20 October 2024, 12:09
[52] Heike Felzmann and others, 'Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns' (2019) 6 Big Data & Society. https://doi.org/10.1177/2053951719860542 accessed 20 October 2024, 12:09
[53] GDPR, art 35. https://gdpr-info.eu/art-35-gdpr/ accessed 20 October 2024, 12:10
[54] Felix Bieker and others, 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' (2016) 4 Privacy Technologies and Policy 21. https://lib.manaraa.com/books/A%20Process%20for%20Data%20Protection%20Impact.pdf accessed 20 October 2024, 12:10

2.2.3 Legal Approaches

Legal strategies of GDPR compliance are mostly concerned with the legal analysis of the regulation and its provisions. These approaches are particularly useful when it comes to the international transfer of personal data because organisations are faced with a set of laws on the transfer of such data. Among the topics that have been primarily discussed in this field are the Standard Contractual Clauses (SCCs) for the transfer of data across borders. Kuner provides a comprehensive analysis of the legal implications that arise concerning the use of SCCs in light of the *Schrems II* decision.[55] He points out that although SCCs are still valid and legal transfer tools, organisations must evaluate each case with regard to the data protection laws of the recipient country to determine a reasonable level of protection. The following are the recommendations for the use of SCCs given by the EDPB after the Schrems II judgement, and very often, supplementary measures are required.[56] This has led to massive literature on how organisations can effectively implement these extra measures to transfer data across borders legally.

Other legal measures include the use of Binding Corporate Rules (BCRs) for the transfers of personal data within the group. Moerel explains how BCRs can serve as a holistic approach to achieving GDPR compliance in the pool of multinational companies despite the fact that the approval process for BCRs can be time-consuming and challenging.[57] She points out that the use of BCRs is less rigid and more feasible than the use of SCCs, especially for large global companies. Another area of investigation in the GDPR has been the territorial reach of the GDPR based on Article 3 of the regulation. Svantesson provides a critical analysis of the GDPR's extraterritorial reach, arguing that while it is necessary to protect EU residents' data in a globalised world, it also creates challenges in terms of enforcement and potential conflicts with other jurisdictions' laws.[58]

---

[55] Christopher Kuner, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (2020) European Law Blog. http://www.kuner.com/my-blog-entries.html accessed 20 October 2024, 12:10

[56] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (10 November 2020). https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en accessed 20 October 2024, 12:11

[57] Lokke Moerel, 'Binding Corporate Rules: Fixing the Regulatory Patchwork of Data Protection' (2011) 28 Chicago Journal of International Law 1. https://pure.uvt.nl/ws/portalfiles/portal/1346784/Moerel_binding_19-09-2011.pdf accessed 20 October 2024, 12:12

[58] Dan Jerker B Svantesson, 'European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce

2.3 Theoretical Frameworks for Data Protection in International Contexts

Several theories have been put forward in order to explain and categorise data protection in the international environment. These frameworks give useful information about the challenges of protecting data across jurisdictions, especially given that the *General Data Protection Regulation* (GDPR) has jurisdictional application.

2.3.1 The Layered Approach

Lee Bygrave's work explores multiple layers of cheques and balances with regard to data protection legislation and regulation.[59] This framework suggests that data protection norms operate at multiple levels: international, regional, national and sub-national. The overlapping of these layers presents a web of regulations that international corporations have to deal with. The layered approach is most appropriate in the case of the General Data Protection Regulation (GDPR), which is an EU regulation but has international consequences because of its extraterritoriality. GDPR Article 3 states the regulation covers EU residents' data processing, whether conducted inside or outside the European Union.[60]

Kuner goes further to explain the layered approach, where he explains that international data protection law is made up of the relationship between multiple legal systems.[61] He argued a 'regulatory maze' emerges from cross-border data transfers, with layered rules creating potential contradictions. This framework maps how regulations interact internationally. Svantesson studies potential conflicts between EU data protection law on the one hand and the law of non-EU countries on the other hand.[62] He also points out that due to the extraterritoriality

---

Law 113. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jipitec9&div=14&id=&page= accessed 20 October 2024, 12:12

[59] Lee A Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014) 31-33. https://doi.org/10.1093/acprof:oso/9780199675555.001.0001 https://heinonline.org/HOL/LandingPage?handle=hein.journals/jipitec9&div=14&id=&page= accessed 20 October 2024, 12:13

[60] 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 L119/1, art 3. https://eur-lex.europa.eu/eli/reg/2016/679/oj https://heinonline.org/HOL/LandingPage?handle=hein.journals/jipitec9&div=14&id=&page= accessed 20 October 2024, 12:16

[61] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013) 125-130. https://doi.org/10.1093/acprof:oso/9780199674619.001.0001 accessed 20 October 2024, 12:15

[62] Dan Jerker B Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stanford Journal of International Law 53. https://heinonline.org/HOL/LandingPage?handle=hein.journals/stanit50&div=6&id=&page= accessed 20 October 2024, 12:16

of the GDPR, organisations may find themselves in conflicting legal requirements – a challenge that requires proportionality when it comes to compliance efforts.

2.3.2 The Principle-Based Approach

Gellert discusses the principle-based approach adopted by the GDPR.[63] This approach focuses on key principles such as lawfulness, fairness, and transparency (Article 5(1)(a) GDPR), purpose limitation (Article 5(1)(b) GDPR), and data minimisation (Article 5(1)(c) GDPR).[64] Gellert has pointed out that this kind of principle-based application is flexible in application across various contexts while at the same time provoking certain problems as to the interpretation of the principles and how they can be implemented. The principle-based approach can be traced to the understanding that technological development and changing business environments may necessitate new rules in a very short time.

The GDPR avoids specifying how technology can be used because it is supposed to be timeless and, thus, can be used in any future technological development. This approach is especially useful as applied to cross-border data flows since it's evident that there are too many technological and organisational environments in the global context to fit into a single rigid mould. The principle-based approach is not without its challenges. As Lynskey points out, the open-ended nature of principles can lead to uncertainty in their practical application.[65] This uncertainty can be particularly problematic for international corporations operating across multiple jurisdictions, each with its interpretation of these principles.

2.3.3 The Risk-Based Approach

The risk-based approach, as discussed by Quelle, is another key theoretical framework underpinning the GDPR.[66] This approach is evident in various provisions of the GDPR, such

---

[63] Raphaël Gellert, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection' (2016) 2 European Data Protection Law Review 481. https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl2&div=83&id=&page= accessed 20 October 2024, 12:17

[64] GDPR, art 5. https://gdpr-info.eu/art-5-gdpr/ accessed 20 October 2024, 12:17

[65] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 89-92. https://books.google.com/books?hl=en&lr=&id=jCXYCgAAQBAJ&oi=fnd&pg=PP1&dq=Orla+Lynskey,+The+Foundations+of+EU+Data+Protection+Law+(Oxford+University+Press+2015)+89-92.&ots=iYe095GzAa&sig=52vR1cHZ-aeBaCp6YJMw8n9oHf4 accessed 20 October 2024, 12:18

[66] Claudia Quelle, 'The 'Risk Revolution' in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too' in Ronald Leenes and others (eds), *Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2018). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000382 accessed 20 October 2024, 12:20

as the requirement for data protection impact assessments (Article 35 GDPR) and the principle of data protection by design and by default (Article 25 GDPR).[67] The risk-based approach requires organisations to assess the potential impacts of data processing on individuals' rights and freedoms and to implement appropriate safeguards based on the level of risk. This approach is especially applicable to cross-border data transfers where the risks to individuals may differ depending on the level of data protection in the state of destination.

Van Alsenoy develops a more risk-based approach, as it enables better adaptation of the data protection rules to the context.[68] He suggests that this approach can help organisations prioritise their compliance efforts, focusing resources on areas of highest risk to data subjects. This risk-based approach has also been unpopular among several individuals. Mantelero points out that overemphasis on risk analysis may contribute to the possible marginalisation of ethical factors in data protection, which is underpinned by a technocratic approach.[69] This critique is particularly relevant in the context of international data flows, where cultural and societal differences may influence perceptions of privacy and data protection risks.

2.3.4 The Accountability Framework

The accountability principle, enshrined in Article 5(2) of the GDPR, has given rise to a theoretical framework focused on demonstrable compliance.[70] Felzmann et al. discuss how the accountability framework shifts the burden of proof onto data controllers, requiring them to demonstrate their compliance with the GDPR actively.[71] This framework is especially suitable for international corporations because, for them to be compliant, they must design and document robust data protection programmes that can be defended in courts by the data protection authorities of various countries. The accountability framework goes beyond mere compliance, encouraging organisations to adopt a proactive approach to data protection. Bennett elaborates on the concept of accountability in data protection, arguing that it

[67] GDPR, arts 25, 35. accessed 20 October 2024, 12:20
[68] Brendan Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 271. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jipitec7&div=28&id=&page= accessed 20 October 2024, 12:22
[69] Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754. https://doi.org/10.1016/j.clsr.2018.05.017 accessed 20 October 2024, 12:24
[70] GDPR, art 5(2). https://gdpr-info.eu/art-5-gdpr/ accessed 20 October 2024, 12:25
[71] Heike Felzmann and others, 'Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns' (2019) 6 Big Data & Society. https://doi.org/10.1177/2053951719860542 accessed 20 October 2024, 12:26

encompasses both internal and external dimensions.[72] Internal accountability refers to the organisational measures and processes put in place to ensure compliance, while external accountability involves demonstrating this compliance to regulators and data subjects.

The accountability framework has significant implications for international data flows. As Kuner points out, organisations engaged in cross-border data transfers must be able to demonstrate compliance with the GDPR's requirements for such transfers, including the implementation of appropriate safeguards.[73] This can be especially trying in the aftermath of the decision in *Schrems II*, in which the Court of Justice of the European Union placed a spotlight on the necessity of country-by-country determinations of the adequacy of protection.

Theoretical concepts are appropriate for analysing and interpreting data protection in the international context. The layered approach promotes the understanding of the rules at different levels; the principle-based approach is suitable for new technologies; the risk-based approach sees situational protections, and the accountability framework provides upfront compliance. They offer a clear reference framework within which issues and approaches concerning GDPR in international data transfers can be studied.

2.4 Key Concepts Related to International Data Flows

Understanding the parameters of transferring data across borders within the GDPR framework requires consideration of several key definitions. These axioms form the basis for evaluating issues and measures related to GDPR in international data transfers. The following section expands on these ideas to provide deeper insight into their impact on international data protection.

2.4.1 Adequacy Decisions

The concept of adequacy decisions, as outlined in Article 45 of the GDPR, is crucial for understanding the legal basis for international data transfers.[74] An adequacy decision rendered

---

[72] Colin J Bennett, 'The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats' in Daniel Guagnin and others (eds), *Managing Privacy through Accountability* (Palgrave Macmillan 2012). http://dx.doi.org/10.1057/9781137032225_3 accessed 20 October 2024, 12:27

[73] Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18 German Law Journal 881. https://doi.org/10.1017/S2071832200022197 accessed 20 October 2024, 12:28

[74] 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 L119/1, art 45 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 accessed 20 October 2024, 12:29

by the European Commission enables transfers of personal data to a third country, a territory or a part of a third country without any authorisation.[75] An adequacy decision is gained through an evaluation of the third country's data protection regime. According to Kuner, such evaluation involves the rule of law and human rights and fundamental freedoms, the legislation, the existence and efficiency of independent supervisory authorities and the international commitments of the country.[76]

As demonstrated by the *Schrems II* case, adequacy decisions are not permanent and can be invalidated if the level of protection in the third country is deemed inadequate.[77] It has massive consequences for the cross-border transfers of data, specifically between the EU and the United States of America. With the annulment of the EU-US Privacy Shield framework in the Schrems II judgement, organisations relying on this mechanism for the transfer of data across the Atlantic have been left in the dark.[78] Kuner argues that the *Schrems II* decision has raised the bar for adequacy, potentially making it more difficult for countries to obtain and maintain adequacy decisions in the future.[79] This could lead to a more fragmented global data protection landscape, with fewer countries meeting the EU's stringent adequacy requirements.

2.4.2 Appropriate Safeguards

In the absence of an adequacy decision, Article 46 of the GDPR allows for international data transfers if appropriate safeguards are in place.[80] These measures may be Standard Contractual Clauses (SCC), Binding Corporate Rules (BCRs), approved codes of conduct or approved certification mechanisms. SCCs, which are baseline contractual clauses for data transfers, have been common means of international data transfers. However, as Nijmann notes, the *Schrems*

[75] European Commission, 'Adequacy decisions' (European Commission) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed 20 October 2024, 12:30
[76] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013) 64-66. https://doi.org/10.1093/acprof:oso/9780199674619.001.0001 accessed 20 October 2024, 12:31
[77] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311 accessed 20 October 2024, 12:33
[78] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (10 November 2020). https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en accessed 20 October 2024, 12:34
[79] Christopher Kuner, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (2020) European Law Blog. http://www.kuner.com/my-blog-entries.html accessed 20 October 2024, 12:35
[80] GDPR, art 46. https://gdpr-info.eu/art-46-gdpr/ accessed 20 October 2024, 12:35

II has made the use of SCCs challenging by asking data exporters to determine whether these clauses afford adequate protection under the laws and practises of the recipient country.[81]

BCRs, on the other hand, are internal transfer rules of a multinational group. According to Moerel, BCRs are both more effective and a more elastic compliance regime for multinationals, even if the approval process can be highly bureaucratic and time-consuming.[82] Especially after the *Schrems II* decision, the idea of appropriate safeguards is becoming more and more crucial, as the Court pointed out that data exporters should determine whether such measures are adequate in the context of the laws and practises of the third country.[83] This requirement has led to heightened attention toward data transfer mechanisms and has forced organisations to put in place further technical, contractual and organisational measures to achieve adequate level of protection of personal data.

2.4.3 Data Localisation

Data localisation refers to the practice of storing data within the borders of a particular country or region. While the GDPR does not explicitly require data localisation, some argue that its strict requirements for international data transfers effectively encourage it.[84] Chander and Lê discuss how data localisation laws in various countries can create significant challenges for international corporations seeking to comply with the GDPR while also meeting local data storage requirements.[85] They argue that data localisation laws can fragment the internet, increase costs for businesses, and potentially undermine data protection by creating multiple points of vulnerability.

---

[81] Laura Bradford, Mateo Aboy and Kathleen Liddell, 'Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II' (2021) 8 Journal of Law and the Biosciences https://doi.org/10.1093/jlb/lsab007 accessed 20 October 2024, 12:36

[82] Elise Marie Leonore Moerel, 'Binding Corporate Rules: Fixing the Regulatory Patchwork of Data Protection' (PhD thesis, Tilburg University 2011) https://research.tilburguniversity.edu/files/1346784/Moerel_binding_19-09-2011.pdf accessed 20 October 2024, 12:37

[83] *Schrems II* (n 4).
https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf accessed 20 October 2024, 12:38

[84] W Kuan Hon, 'Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens' (Edward Elgar Publishing 2017).
https://books.google.com/books?hl=en&lr=&id=hVXYDgAAQBAJ&oi=fnd&pg=PR1&dq=W+Kuan+Hon,+%27Data+Localization+Laws+and+Policy:+The+EU+Data+Protection+International+Transfers+Restriction+Through+a+Cloud+Computing+Lens%27+(Edward+Elgar+Publishing+2017).&ots=bML6dlomXS&sig=3Y797b-XmFA25LjmpZgQAKkY1iY accessed 20 October 2024, 12:39

[85] Anupam Chander and Uyên P Lê, 'Data Nationalism' (2014) 64 Emory Law Journal 677.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/emlj64&div=32&id=&page= accessed 20 October 2024, 12:40

The tension between data localisation and the free flow of data is particularly evident in the context of cloud computing. Hon and Millard look at the difficulties of attempting to localise data in the context of the global and centralised services of cloud computing while also pointing out that the current approach to data protection is inadequate for the current technologies used in data processing.[86]

2.4.4 Extraterritorial Scope

The extraterritorial scope of the GDPR, as defined in Article 3, is a key concept that has significant implications for international data flows.[87] This provision of the GDPR expands the geographical scope of the regulation to organisations outside the EU who deal with personal data of individuals within the EU insofar as it relates to the supply of goods and services or profiling of the individuals. Svantesson argues that while the extraterritorial scope of the GDPR is necessary to protect EU residents' data in a globalised world, it also creates challenges in terms of enforcement and potential conflicts with other jurisdictions' laws.[88] He points out that the vast geographical scope of the GDPR may cause juridical over-assertiveness and infringement on the sovereignty of other countries.

The extraterritorial scope of the GDPR has far-reaching implications for international businesses. As Azzi points out, it effectively requires many non-EU organisations to comply with EU data protection standards, potentially leading to a de facto globalisation of EU data protection norms.[89] This phenomenon, often referred to as the "Brussels effect," has been extensively analysed by Bradford, who argues that the EU's regulatory power extends well beyond its borders through market mechanisms.[90] The practical enforcement of the GDPR's

---

[86] W Kuan Hon and Christopher Millard, 'Banking on the Cloud: Effects of Security, Privacy and Data Protection Laws on Cloud Use' (2018) 15 Journal of International Commercial Law and Technology 1. https://doi.org/10.1016/j.clsr.2017.11.005 accessed 20 October 2024, 12:41

[87] GDPR, art 3. https://gdpr-info.eu/art-3-gdpr/ accessed 20 October 2024, 12:42

[88] Dan Jerker B Svantesson, 'European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 113. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jipitec9&div=14&id=&page= accessed 20 October 2024, 12:44

[89] Adèle Azzi, 'The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 126. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jipitec9&div=15&id=&page= accessed 20 October 2024, 12:45

[90] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020). https://books.google.com/books?hl=en&lr=&id=mZXHDwAAQBAJ&oi=fnd&pg=PP1&dq=Anu+Bradford,+The+Brussels+Effect:+How+the+European+Union+Rules+the+World+(Oxford+University+Press+2020).&ots=D_0mITZSHK&sig=lNu2BW6Yw_muGZfGKVWmPqxiRBA accessed 20 October 2024, 12:46

extraterritorial provisions remains a challenge. Greze discusses the complexities of enforcing the GDPR against non-EU entities, highlighting the need for international cooperation and the potential role of private enforcement mechanisms.[91]

These key concepts - adequacy decisions, appropriate safeguards, data localisation, and extraterritorial scope - form the cornerstones of the GDPR's approach to international data flows. They show that the regulation was made in order to reconcile the protection of personal data with the requirements of the rapidly growing digital economy on an international level. Knowledge of these ideas is useful for organisations that deal with the international data protection environment, as they define the legal and practical context of the cross-border data transfers in nowadays GDPR world.

2.5 Research Gap

Despite the growing body of literature on *General Data Protection Regulation* (GDPR) compliance and international data flows, several significant research gaps remain. These gaps define the empirical focus of the present study and stress the importance of ongoing research in this field. This section will explore these gaps and explain the state-of-the-art aspects that require further investigation to understand and manage the difficulties implied by GDPR enforcement in the context of international data transfers.

2.5.1 Lack of Comprehensive Studies on Practical GDPR Compliance Strategies

Although there are countless empirical papers on various aspects of GDPR compliance, there are no studies that combine technical, organisational, and legal perspectives on compliance, especially when it comes to multinational companies. According to Tikkinen-Piri et al., most of the previous works are centred around individual compliance indicators instead of offering an overall picture of the GDPR compliance plans.[92]

This gap is especially apparent when focusing on the real-life issues that multinational companies encounter when trying to bring their GDPR compliance into practice across

[91] Benjamin Greze, 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives' (2019) 9 International Data Privacy Law 109. https://doi.org/10.1093/idpl/ipz003 accessed 20 October 2024, 12:47

[92] Christina Tikkinen-Piri, Anna Rohunen and Jouni Markkula, 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 Computer Law & Security Review 134. https://doi.org/10.1016/j.clsr.2017.05.015 accessed 20 October 2024, 12:47

countries. There is a dearth of research that not only points to potential compliance strategies but also gives insight into the efficacy of these strategies in practise. As Voigt and von dem Bussche point out, the complexity of the GDPR and its broad scope necessitates a multifaceted approach to compliance that considers technical, organisational, and legal aspects in an integrated manner.[93] The interplay between these different aspects of compliance remains underexplored. For instance, how do technical measures like encryption interact with organisational policies and legal safeguards to ensure comprehensive GDPR compliance? Research addressing these questions could provide valuable insights for international corporations seeking to develop robust compliance strategies.

2.5.2 Limited Research on Challenges Across Different Jurisdictions

While the GDPR has global implications, research on its impact across different jurisdictions remains limited. As highlighted by Kuner, there is a need for more comparative studies that examine how the GDPR interacts with data protection regimes in non-EU countries.[94]

This research gap is especially important because the legal environment of international business is rather intricate. Assessing the need for GDPR compliance across multiple jurisdictions that have different laws, regulations and practices for implementing those laws is important for finding ways to cope with the problem. Svantesson also points out that the GDPR's application beyond the territory of the Member States generates potential clashes with the laws of other jurisdictions, while the consequences of these clashes are still understudied.[95]

2.5.3 Need for Analysis of Schrems II Decision's Implications

The *Schrems II* decision by the Court of Justice of the European Union (CJEU) in July 2020 has had far-reaching implications for international data transfers.[96] Although much has been

---

[93] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017). http://dx.doi.org/10.1007/978-3-319-57959-7 accessed 20 October 2024, 12:48

[94] Christopher Kuner, 'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (OUP 2017) 112 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890930 accessed 20 October 2024, 12:48

[95] Dan Jerker B Svantesson, 'European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 113. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jipitec9&div=14&id=&page= accessed 20 October 2024, 12:49

[96] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311 accessed 20 October 2024, 12:50

written and said on the effect of this decision, especially on EU-US data transfers, there is a dearth of detailed analysis of the potential consequences of this decision.

More generally, there remains a gap in the literature on how the standards set by the CJEU in *Schrems II* extend to transfers of data from the EU to the rest of the world, not only the US. This gap in understanding poses significant challenges for international corporations seeking to ensure GDPR compliance in their global data transfer practices. As Kuner points out, the *Schrems II* decision has raised the bar for what constitutes adequate protection, potentially affecting data transfers to many countries beyond the US.[97] Research is needed on the practical implications of the supplementary measures required by *Schrems II*. How can organisations effectively implement and demonstrate the efficacy of these measures? What are the technical, organisational, and legal challenges involved? These questions remain largely unanswered and represent a significant gap in the current literature.

2.5.4 Limited Empirical Research on GDPR Compliance in International Corporations

Theoretical research on GDPR compliance is emerging, yet empirical studies illuminating how international organisations implement GDPR requirements remain scarce. Gellert highlights the lack of qualitative case research exploring actual GDPR practices in multinational companies.[98] This gap is especially acute in the context of the sophisticated organisational structure of international corporations and the heterogeneity of data processing procedures. How exactly these organisations modify their activities to fit the GDPR standards throughout different countries could be of interest for the theory and practise. Moerel explains that the practices of multinational corporations in the adoption of global privacy programmes can have valuable lessons in building an international data protection regime.[99]

Further qualitative research could reveal how organisations circumvent GDPR and what pitfalls they have encountered, providing lessons and recommendations for other organisations and

---

[97] Christopher Kuner, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (2020) European Law Blog. http://www.kuner.com/my-blog-entries.html accessed 20 October 2024, 12:51

[98] Raphaël Gellert, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection' (2016) 2 European Data Protection Law Review 481. https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl2&div=83&id=&page= accessed 20 October 2024, 12:52

[99] Elise Marie Leonore Moerel, 'Binding Corporate Rules: Fixing the Regulatory Patchwork of Data Protection' (PhD thesis, Tilburg University 2011) https://research.tilburguniversity.edu/files/1346784/Moerel_binding_19-09-2011.pdf accessed 20 October 2024, 12:53

future legislative measures. Such research could also illuminate which compliance strategies effectively reduce misconduct in practice, offering insight into the gap between compliance theory and practice.

2.5.5 Insufficient Research on the Interplay Between GDPR and Emerging Technologies

The rapid pace of technological advancement presents ongoing challenges for data protection. While some research has examined the implications of the GDPR for technologies such as artificial intelligence and blockchain, there is a need for more comprehensive studies on how international corporations can ensure GDPR compliance while leveraging these emerging technologies.[100]

This gap is particularly relevant given the global nature of many technological developments and the potential for these technologies to facilitate or complicate international data flows. As Finck points out, technologies like blockchain can present unique challenges for GDPR compliance, particularly in areas such as data minimisation and the right to erasure.[101] The use of artificial intelligence and machine learning in data processing raises complex questions about transparency, explainability, and fairness that are not fully addressed by current research. How can organisations ensure GDPR compliance when using these technologies for cross-border data processing? What new risks do these technologies introduce, and how can they be mitigated? These questions represent significant gaps in the current understanding of GDPR compliance in the context of emerging technologies.

2.6 Conclusion

This literature review has highlighted the current work done on GDPR compliance approaches, the theoretical work done for data protection in the global environment and some of the vital terms used in the international transfer of data. It has also provided suggestions for future research with regard to compliance strategies for international corporations, matters in various countries, and impacts of the *Schrems II* judgement. Such gaps indicate the need for more research that can give a more general picture of how international corporations approach GDPR

[100] Luca Tosoni, 'The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation' (14 May 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3845913 accessed 20 October 2024, 12:54

[101] Michèle Finck, 'Blockchains and Data Protection in the European Union' (2018) 4 European Data Protection Law Review 17. https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl4&div=8&id=&page= accessed 20 October 2024, 12:55

compliance in their international data transfers. In search of answers to these questions, this thesis aims to provide a theoretical contribution to the topic of international data protection as well as a practical contribution in the form of heuristic insights for GDPR compliance in multinational organisations.

Chapter 3: Research Methodology

3.1 Introduction

This chapter presents the research process employed in this thesis to identify the strategies and challenges that international corporations face concerning the management of personal data flow as per the GDPR. The methodology is designed to respond to the research questions and the hypotheses outlined in Chapter 1 related to the effect of the *Schrems II* decision on international data flow practises. The study adopts a qualitative research approach in which doctrinal legal research methods predominate and are supported by comparative analysis. It is particularly suitable for shaping the principles of data protection law, a new and still dynamically evolving branch of law, and for furthering its consideration in the international process.[102]

3.2 Research Questions and Hypotheses

The methodology is structured to address three key research questions.

(1) Primary question: How do internationally operating corporations manage the flow of personal data to ensure compliance with GDPR regulations?
(2) Secondary question 1: What are the key challenges faced by internationally operating corporations in maintaining GDPR compliance across different jurisdictions?
(3) Secondary question 2: What are the implications of the *Schrems II* decision on the international data flow practices of internationally operating corporations?

Three hypotheses underpin these questions.

[102] Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17(1) Deakin Law Review 83, 85. https://search.informit.org/doi/pdf/10.3316/agis_archive.20125043 accessed 21 October 2024, 09:10

(1) International corporations adopt a range of strategies to manage GDPR compliance, including technical, organisational, and legal measures.
(2) Key challenges include varying legal standards, enforcement practices across jurisdictions, and operational complexities.
(3) The *Schrems II* decision is profound and has put the corporations in a new position where they must now review and optimise their data transfer practises.

3.3 Research Design

The primary method employed in this thesis is doctrinal legal research, which involves a systematic analysis of legal rules, principles, and judicial decisions.[103] This method is suitable to use to analyse the complex legislation regarding the GDPR and international data processing. The doctrinal analysis will be made according to the text of the GDPR, particularly Chapter V concerning the transfers of personal data to third countries or international organisations.[104] The analysis will also consider the interaction between GDPR and other major data protection frameworks, such as the California Consumer Privacy Act (CCPA).[105]

To provide concrete examples of the strategies and challenges faced by international corporations, this research will incorporate a case study approach. This will entail reviewing public disclosures of compliance with data protection laws and regulations, as well as general statements by large multinationals on compliance with GDPR and data protection laws in cross-border contexts, surveying the data protection incidents and enforcement actions relating to international transfers, and surveying the industry practises and standards for GDPR compliance in the international environment. This approach will assist in humanising the theoretical and legal framework and useful for understanding how GDPR compliance strategies are implemented.[106]

---

[103] Mark Van Hoecke, 'Legal Doctrine: Which Method(s) for What Kind of Discipline?' in Mark Van Hoecke (ed), *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Hart Publishing 2011) 1. https://lib.ugent.be/catalog/pug01:1091776 accessed 21 October 2024, 09:11
[104] 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 L119/1, ch V. https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed 21 October 2024, 09:13
[105] Anupam Chander, Margot E Kaminski and William McGeveran, 'Catalyzing Privacy Law' (2021) 105 Minnesota Law Review 1733. https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=4353&context=mlr accessed 21 October 2024, 09:18
[106] Robert K Yin, *Case Study Research and Applications: Design and Methods* (6th edn, SAGE Publications 2017). https://www.academia.edu/download/106905310/Artikel_Yustinus_Calvin_Gai_Mali.pdf accessed 21 October 2024, 09:20

3.4 Data Collection and Analysis

Sources of data for this research will include legal instruments and documents, peer-reviewed articles, compliance and industry reports, and news articles and press releases. The discussion shall focus at comparing and contrasting all the provisions of the GDPR and other EU legislation regarding protection of personal data, Court of Justice of the European Union (CJEU) and national case laws. European Data Protection Board (EDPB) opinions and views from the national data protection authorities will also be compared and the legislation texts of the data protection laws of selected non-EU member states. The collected data will be analyzed through a qualitative analysis of research. Legal analysis will be used to determine explicit legal provisions within the GDPR regarding transfers of data internationally, understand the legal basis for some of the determinations made in the legislation, and decipher legal and judicial decisions for international business entities. This analysis will use conventional legal doctrinal research, such as statutory construction, and case studies.[107]

Legal analysis will be used to examine academic literature, court cases, industry reports, and other collected materials. This will entail reviewing legal texts, judicial precedents, and official standards to determine that there are express legal requirements within the GDPR; to determine how they are implemented and to explain legal rulings that impact on international business.[108] It will assist in understanding some broad patterns of the approaches used by the global business organisations to meet the requirements of GDPR, ascertain the persistent issues in GDPR compliance across borders, and distinguish novel trends and practises concerning the international data transfers. In analysing the data on various jurisdictions' approach to data protection, comparative analysis will be used. This will focus on comparison of legal compliance and penalties associated with it, and the legal and enforcement disparities that will be the cause of understanding the issues of compliance with GDPR in other regions that have different legal standards and how they may conflict with GDPR. This approach will assist in placing the difficulties of the international business operating in different regulatory systems.[109]

---

[107] Ian McLeod, *Legal Method* (10th edn, Palgrave Macmillan 2019) ch 5. https://mguntur.id/files/ebook/ebook_1605607370_cc240cedb9a1c617d0fe.pdf accessed 21 October 2024, 09:25

[108] Virginia Braun and Victoria Clarke, 'Using thematic analysis in psychology' (2006) 3(2) Qualitative Research in Psychology 77. https://www.tandfonline.com/doi/abs/10.1191/1478088706QP063OA accessed 21 October 2024, 09:26

[109] Mathias Siems and Po Jen Yap (eds), *The Cambridge Handbook of Comparative Law* (CUP 2024) https://books.google.com/books?id=TdPvEAAAQBAJ accessed 21 October 2024, 09:27

3.5 Ethical Considerations and Limitations

While this research primarily relies on publicly available documents and does not involve human subjects, ethical considerations remain important. The research will adhere to principles of accuracy and integrity in the representation of legal provisions and scholarly works, transparency in the research process, respect for intellectual property rights, and impartiality in the analysis.

It should be borne in mind that some of the findings may, in the future, become obsolete due to the dynamism that characterises the field of data protection law. In order to avoid this, the research will be based on principles and trends rather than temporary arrangements. One of the major drawbacks of this approach is that the analysis can only rely on information from outside of corporations and therefore may ignore their internal compliance. This limitation is recognised, and conclusions will be stated with necessary caveats. This kind of systematization of the regulation of interstate data protection may contribute to uncertainty and contradictory conclusions. The research will aim to provide a nuanced understanding rather than oversimplified solutions. Finally, the focus on EU law and the GDPR may limit the generalisability of findings to other jurisdictions. Where possible, the research will draw broader principles applicable beyond the EU context.

3.6 Conclusion

This methodology has been designed to provide a comprehensive and rigorous examination of the strategies and challenges faced by international corporations in managing GDPR compliance for international data flows. By combining doctrinal legal research with comparative analysis and case studies, the research aims to offer both theoretical insights and practical understanding of this complex area of law and business practice. The outcomes arising from this approach will be discussed in the subsequent chapters of the work, as well as answers to the research questions and test the hypothesised relations. The above approach shall assist in the enhancement of understanding of GDPR measures concerning the transfer of data across borders with emphasis on the impacts of the *Schrems II* ruling.

Chapter 4: GDPR Compliance Strategies in International Corporations

4.1 Introduction

The GDPR has fundamentally altered data protection for international corporations managing cross-border data flows.[110] This chapter examines organisations' approaches to meeting GDPR requirements, including technical, organisational, and legal solutions, with case studies from leading companies. Multinational companies face challenges due to the GDPR's extraterritorial application (Article 3)[111] and restrictions on international data transfers (Chapter V),[112] necessitating a holistic approach to data protection. The *Schrems II* judgment[113] further complicates compliance efforts. These challenges require global businesses to develop adaptable compliance regimes addressing legal evolution and best practices.

4.2 Technical Measures

Technical measures are the most important element of GDPR compliance programmes as they offer the technical support needed for the protection of data and the legal and proper processing of such information. They are especially important for global businesses that deal with flows of data across borders and jurisdictions. The application of strict technical requirements also guarantees compliance with the GDPR while also strengthening customer and partner confidence in the company's adherence to data protection standards.

4.2.1 Encryption and Pseudonymisation

Encryption and pseudonymisation are explicitly mentioned in the GDPR as appropriate technical measures to ensure data security and compliance.[114] Encryption covers data into a code to avoid accessibility by unauthorised parties, while pseudonymisation substitutes information containing identity with artificial identifiers. These techniques are basic to warrant the integrity of personal data and prevent incidents of data breaches. International corporations have widely implemented these techniques for data in transit as well as data at rest. For instance, Microsoft uses encryption on user's data and data in transit in the Microsoft data centres and

---

[110] 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 L119/1. https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed 21 October 2024, 09:28

[111] ibid art 3.

[112] ibid ch V.

[113] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311 accessed 21 October 2024, 09:30

[114] 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 L119/1, art 32. https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed 21 October 2024, 09:30

encryption of data transferring from one datacenter to another.[115] This approach helps mitigate risks associated with international data transfers, a key concern following the *Schrems II* decision.[116] End-to-end encryption guarantees that data is safe even if it is captured during transfer by some unauthorised person.

Pseudonymisation has become popular as a method that enables data use while improving privacy. In Google Analytics service, the user ID is substituted with a pseudonymous identifier before the data is processed.[117] This approach enables Google to give meaningful information to its international clients without the possibility of identifying individual users. The application of pseudonymisation allows organisations to meet their analytical requirements while protecting the rights of individuals, which is a GDPR. The European Data Protection Board (EDPB) guidance recommends encryption and pseudonymisation for international data transfers, alongside additional measures to ensure EU-equivalent protection levels.[118]

4.2.2 Data Minimisation and Purpose Limitation Technologies

Data minimisation and purpose limitation are both principles of the GDPR enshrined in Article 5, whereby organisations must only collect and process data that is necessary for the specified, explicit and legitimate purpose.[119] International companies have adopted various technical methods to apply GDPR principles effectively. Data discovery and categorisation technologies have become essential for identifying personal information within complex IT systems. These tools enable organisations to map data storage and processing locations – vital information for implementing data minimisation strategies. Access control systems are crucial for enforcing purpose limitations. Granular controls ensure only authorised personnel can access specific datasets. Multinational corporations commonly implement role-based access control (RBAC) and attribute-based access control (ABAC) to achieve GDPR compliance.

---

[115] Microsoft, 'Encryption in the Microsoft Cloud' (Microsoft Trust Center, 2024). https://learn.microsoft.com/en-us/purview/office-365-encryption-in-the-microsoft-cloud-overview accessed 21 October 2024, 09:31

[116] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian *Schrems* [2020] ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311 accessed 21 October 2024, 09:32

[117] Google, 'Data Processing Amendment to Google Analytics Terms of Service' (Google, 2024) https://support.google.com/analytics/answer/3379636 accessed 21 October 2024, 09:34

[118] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (10 November 2020). https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en accessed 21 October 2024, 09:36

[119] GDPR (n 1) art 5. https://gdpr-info.eu/art-5-gdpr/ accessed 21 October 2024, 09:36

Additionally, retention and deletion tools support the storage limitation principle. IT solutions for controlling the retention of data and erasing data when it is not required any longer offer compliance with this principle. These tools typically contain configurable elements like data lifecycle management, methods of data elimination that are secure, and records of compliance. The American cloud service provider Amazon Web Services (AWS), which hosts companies around the world, provides functions such as Amazon Macie for data identification and Amazon Identity and Access Management for individual access permissions. [120] These technologies help AWS customers apply data minimisation and purpose limitation principles systematically in their operations worldwide. The incorporation of such tools into the cloud infrastructure services should show the increasing awareness of privacy enhancing technologies in the global IT environment.

4.2.3 Data Protection Impact Assessment (DPIA) Tools

The GDPR mandates Data Protection Impact Assessments (DPIAs) for high-risk processing activities.[121] To optimise this process, global businesses have designed specific instruments that include risk assessment matrices, computerised questionnaires, compliance checklists, and database links. These automated solutions allow organisations to systematically evaluate risks to individuals' rights and freedoms arising from data processing activities while maintaining coherence in documentation.

Systems, Applications and Products in Data Processing (SAP AG), a multinational software corporation, has integrated a DPIA tool within its product development lifecycle. [122] This integration enables evaluation of data protection impact for new products and features at conception, applying consistently worldwide. This implementation demonstrates privacy by design as mandated under Article 25 of the GDPR.[123] Such systematic approaches reflect a growing appreciation of risk evaluation in data security while increasing organisational privacy awareness and GDPR compliance.

---

[120] Amazon Web Services, 'AWS Compliance' (AWS) https://aws.amazon.com/compliance/ accessed 21 October 2024, 09:37
[121] GDPR (n 1) art 35. https://gdpr-info.eu/art-35-gdpr/ accessed 21 October 2024, 09:39
[122] SAP, 'SAP's Data Protection Impact Assessment Tool' (SAP Trust Center, 2024) https://www.sap.com/about/trust-center/data-protection-and-privacy.html accessed 21 October 2024, 09:40
[123] GDPR (n 1) art 25. https://gdpr-info.eu/art-25-gdpr/ accessed 21 October 2024, 09:44

4.2.4 Cross-border Data Transfer Technologies

The challenges arising from the *Schrems II* decision have encouraged organisations to look for technologies that would enable legal cross-border data transfers. These technologies seek to meet the objections made by the Court of Justice of the European Union on the transfer of personal data outside the EU. Data localisation technologies have gained prominence as a means of ensuring that data is stored and processed within specific geographic regions. These tools enable organisations to maintain control over the physical location of their data, addressing concerns about data access by foreign governments. To meet this demand, cloud service providers have introduced the geographical availability of data storage and data localisation commitments.

The necessity of carrying out case-by-case assessments of data transfers has given rise to data transfer impact assessment tools as a result of *Schrems II*. Such automated systems assist organisations in assessing the risks related to particular transfers of data, taking into account the type of data, the legal regime of the country of import, and protection measures. International data transfer security has been enhanced through the development of secure means of data transfer. Such protocols may include today's high level of encryption, identity and access control, as well as continuous monitoring of the system for potential intruders.

IBM has developed its data privacy and security services that provide its clients with data discovery, protection, and compliant transfer across borders.[124] These technologies help IBM's multinational clients navigate the complex landscape of international data protection regulations. The development of such comprehensive data protection suites reflects the growing market for privacy-enhancing technologies in the wake of stringent data protection regulations. The implementation of these cross-border data transfer technologies demonstrates the ongoing efforts of international corporations to adapt to the evolving regulatory landscape. As data protection authorities continue to scrutinise international data flows, the role of these technologies in ensuring GDPR compliance is likely to become increasingly significant.

4.3 Organisational Measures

[124] IBM, 'IBM Data Privacy Services' (IBM, 2024) https://www.ibm.com/data-privacy accessed 21 October 2024, 09:47

While technical measures provide the infrastructure for GDPR compliance, organisational measures ensure that these technologies are effectively implemented and integrated into business processes. These measures encompass policies, procedures, and structural changes within corporations. The implementation of robust organisational measures is crucial for creating a culture of data protection and ensuring consistent application of GDPR principles across global operations.

4.3.1 Appointment of Data Protection Officers (DPOs)

According to the GDPR Article 37, Data Protection Officers (DPOs) must be appointed by specific types of organisations that process personal data, including those whose processing activities include large-scale processing of special categories of data or the processing of data in relation to large-scale and regular monitoring of data subjects.[125] In most cases, global organisations hire Data Protection Officers for their data protection strategies, even when they are not legally bound to. The appointment of the DPO also indicates an organisation's compliance with data protection laws. Also, DPOs act as the reference points for handling all the issues of privacy in organisations.

The DPO has many expansive and significant responsibilities in order to guarantee the GDPR compliance. DPOs are supposed to report on noncompliance with the GDPR and other data protection laws, to give recommendations on Data Protection Impact Assessments, to serve as a spokesperson to data subjects and supervisory authorities, and to provide informatin of data protection in the design and by default. The Article 29 Working Party has provided detailed guidance on the role of DPOs, emphasising their independence and the need for direct reporting to the highest management level.[126]

Deutsche Telekom has established a comprehensive DPO structure across its global operations. The Group Data Protection Officer coordinates a network of local DPOs, ensuring consistent application of data protection principles across the corporation's international subsidiaries.[127]

---

[125] 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 L119/1, art 37. https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed 21 October 2024, 09:49

[126] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ('DPOs')' (WP 243 rev.01, 5 April 2017). https://ec.europa.eu/newsroom/just/document.cfm?doc_id=44100 accessed 21 October 2024, 09:50

[127] Deutsche Telekom, 'Data Privacy' (Deutsche Telekom, 2024) https://report.telekom.com/interim-report-q2-2024/services/privacy-policy.html accessed 21 October 2024, 09:51

This approach demonstrates how large multinational corporations can implement a centralised yet locally responsive data protection strategy. The appointment of DPOs in international corporations has led to the development of new professional roles and career paths in data protection. Organisations such as the European Institute of Public Administration (EIPA) have developed specialised training programs for DPOs, contributing to the professionalisation of this role.[128]

4.3.2 Employee Training and Awareness Programs

Effective GDPR compliance requires a culture of data protection throughout the organisation. Many international corporations have implemented comprehensive training programs to ensure all employees understand their responsibilities under the GDPR. These training programs are essential for translating legal requirements into practical, day-to-day behaviours and decisions. Employee training programmes cover the fundamental principles of the GDPR and data subjects' rights. These programmes include comprehensive guidance on data breach procedures. Role-specific guidance is provided for employees handling sensitive data. These programmes are developed with the understanding that data protection responsibilities are not the same across departments in the organisations.

Using Telefónica as an example, one of the largest global telecommunications companies, it has established a data protection and privacy training with is compulsory for all provedors globally, and is updated periodically to ensure we take into account new rules of the laws of data protection as well as changes in best practices..[129] The company's approach demonstrates the importance of ongoing education in maintaining GDPR compliance, particularly in a rapidly evolving regulatory landscape. Research conducted by the European Union Agency for Cybersecurity (ENISA) has shown that effective training programs can significantly reduce the risk of data breaches caused by human error.[130] As such, investment in employee training is increasingly seen not just as a compliance requirement but as a key risk management strategy.

---

[128] European Institute of Public Administration, 'Data Protection Officer (DPO) Certification Training' (EIPA, 2024) https://www.eipa.eu/courses/data-protection-certification/ accessed 21 October 2024, 09:53

[129] Telefónica, 'Global Privacy Policy' (Telefónica, 2021) https://www.telefonica.com/en/wp-content/uploads/sites/5/2021/03/global-privacy-policy.pdf accessed 21 October 2024, 09:57

[130] European Union Agency for Cybersecurity, 'Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity' (ENISA, December 2023). https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity accessed 21 October 2024, 09:59

4.3.3 Data Protection Policies and Procedures

International corporations have developed and implemented a range of policies and procedures to ensure consistent application of GDPR principles across their global operations. These policies and procedures are practical implementations of the general GDPR guidelines at the employee and system level. Policies can be defined as general documents that define the organisation's approach to data protection. GDPR compliance includes having proper procedures regarding data breach responses. These procedures provide an outline of how to identify, report and prevent data breaches. The 72-hour breach notification has become imperative under the GDPR and, therefore, calls for clear and tested breach response plans.[131] Request handling procedures describe how an organisation deals with requests from data subjects exercising their GDPR rights, for example, the right to access, to rectification or the right to erasure. Such procedures usually entail the integration of various departments and systems, hence the establishment of work procedures and duties.

Records retention and disposal policies indicate how long certain kinds of data should be kept and when they should be destroyed. These policies are important for implementing the GDPR's storage limitation principle and sometimes might involve a consideration of numerous legal and business factors regarding data storage. Royal Dutch Shell has a well-developed set of organisational privacy policies and guidelines that are applicable to its operations internationally. These are a Global Data Privacy Policy, a Cookie Notice and a detailed process for dealing with the data subject's request.[132] Shell's approach shows that global policies can be applied uniformly across different markets and business divisions.

4.3.4 Privacy Governance Structures

Global organisations establish privacy frameworks to coordinate GDPR compliance, enabling structured data protection decision-making and oversight. Privacy steering committees are often established as cross-functional groups overseeing the organisation's privacy strategy. These committees typically include representatives from legal, IT, security, HR, and key

[131] Information Commissioner's Office, 'Data Security Incident Trends' (ICO, Q3 2023-24) https://ico.org.uk/action-weve-taken/data-security-incident-trends/ accessed 21 October 2024, 10:01
[132] Royal Dutch Shell, 'Privacy Policy' (Shell, 2024) https://www.mesc.shell.com/Content/HTML%20pages/PrivacyPolicy.html accessed 21 October 2024, 10:05

business units. They play a crucial role in setting privacy priorities, allocating resources, and ensuring that privacy considerations are integrated into business strategies.[133]

The concept of privacy champions has gained traction in many organisations. These are designated individuals within different business units responsible for promoting privacy best practices. Privacy champions act as a bridge between the central privacy function and local operations, helping to embed privacy considerations into day-to-day activities. Regular privacy audits and assessments are essential components of privacy governance. Systematic privacy assessments help organisations identify gaps, track progress, and demonstrate GDPR accountability. [134] Nestlé's Global Privacy Program exemplifies effective centralised governance for privacy management across diverse markets and product lines in a multinational environment.[135] The implementation of privacy governance structures reflects a broader trend towards treating data protection as a board-level issue. Research conducted by the Centre for Information Policy Leadership has shown that organisations with mature privacy governance structures are better equipped to navigate the complexities of global data protection regulations and to respond effectively to data protection challenges.[136]

4.4 Legal Measures

Legal measures form a crucial component of GDPR compliance strategies for international corporations, providing the contractual and procedural frameworks necessary for lawful data processing and transfer. These measures are essential for ensuring that data flows across borders comply with the stringent requirements of the GDPR, particularly in light of recent legal developments that have reshaped the landscape of international data transfers.

---

[133] Ibid 132.
[134] European Data Protection Supervisor, 'Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies' (EDPS, 16 July 2019). https://www.edps.europa.eu/sites/default/files/publication/19-07-17_summary_accountability_guidelines_en.pdf accessed 21 October 2024, 10:05
[135] Nestlé, 'Privacy Notice' (Nestlé, 2024) https://www.nestle.com/info/privacy/privacy-notice accessed 21 October 2024, 10:06
[136] 'CIPL Issues White Paper on GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges' (Hunton Andrews Kurth Privacy & Information Security Law Blog, 6 June 2019) https://www.huntonak.com/privacy-and-information-security-law/cipl-issues-white-paper-on-gdpr-one-year-in-practitioners-take-stock-of-the-benefits-and-challenges accessed 21 October 2024, 10:07

4.4.1 Standard Contractual Clauses (SCCs)

Standard Contractual Clauses (SCCs) have become a primary mechanism for ensuring adequate protection of personal data transferred outside the EU, especially following the invalidation of the EU-US Privacy Shield by the *Schrems II* decision. The European Commission has released new SCCs that should help to counter the issues that arose in the *Schrems II* case.[137] These new SCCs are used in data transfer contracts by international corporations to a large extent. SAP, for instance, has modified its data processing agreements to include the new SCCs as a legal tool for giving contractual structure to data transfers to and from SAP's international cloud services.[138] The Schrems II decision revealed SCCs' insufficiency, especially for transfers to countries lacking robust data protection laws. This has prompted corporations to enhance their SCCs with additional technical controls or data residency options.

The EDPB's guidance on further protection measures emphasises a case-by-case assessment of adequacy, reinforcing the role of SCCs in monitoring cross-border data transfers while adhering to EU data protection laws.[139] The application of SCCs with secondary measures has introduced new challenges for international organisations, particularly in assessing data protection risks in recipient countries. This has spurred the development of enhanced tools and services for such assessments, indicating evolving compliance measures in international data transfers.[140]

4.4.2 Binding Corporate Rules (BCRs)

Binding Corporate Rules (BCRs) provide another legal basis for intra-group transfers of personal data outside the EU. BCRs are internal policies of multinational groups of companies

---

[137] 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 L199/31. https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj accessed 21 October 2024, 10:08

[138] SAP, 'Data Processing Agreement for SAP Cloud Services' (SAP Trust Center, 2024) https://www.sap.com/africa/about/trust-center/agreements/on-premise/data-processing-agreements.html accessed 21 October 2024, 10:09

[139] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (18 June 2021). https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en accessed 21 October 2024, 10:11

[140] OneTrust, 'Schrems II Solutions' (OneTrust, 2024) https://www.onetrust.com/solutions/schrems-ii-compliance/ accessed 21 October 2024, 10:13

that regulate the international transfer of data within the same corporate group.[141] They provide a full-spectrum and adaptable solution for compliance with the GDPR within large and diverse organisations. Although the process of obtaining approval for BCRs might take a considerable amount of time and effort, this approach is widely used by many large international companies and organisations because of its comprehensive and adaptable character. For example, Novartis has global BCRs, which regulate intra-group transfer of personal data across all the entities in the company.[142] BCRs help large organizations develop consistent personal data protection practices globally.

Privacy principles that are usually found within BCRs include things such as transparency, data quality and security, tools for effectiveness, which may include training and audit programmes and evidence showing that the rules are enforceable both internally and externally. As for the legal requirements, the creation and the adoption of BCRs make an organisation review and improve its data protection policies to meet the GDPR standards.[143] The European Data Protection Board has elaborated the guidelines for the BCRs and has stressed that they should be legally enforceable for all the members of the group.[144]

4.4.3 Data Processing Agreements

The GDPR requires controllers to have a contract or other legal act in place with processors outlining the specifics of the data processing activities.[145] Multinationals may be both controllers and processors of personal data, which creates the need for a plethora of data processing contracts. They are of central importance in shaping the relationships and setting up mechanisms of liability in data processing arrangements. Data processing agreements typically

---

[141] Article 29 Data Protection Working Party, 'Working Document Setting Up a Table with the Elements and Principles to be Found in Binding Corporate Rules' (WP 256 rev.01, 6 February 2018). https://ec.europa.eu/newsroom/article29/redirection/document/49725 accessed 21 October 2024, 10:15

[142] Novartis, 'Binding Corporate Rules' (Novartis, 2024) https://www.novartis.com/privacy#:~:text=To%20complement%20the%20Novartis%20Policy,is%20governed%20by%20the%20EU accessed 21 October 2024, 10:16

[143] Bird & Bird, 'Guide to the General Data Protection Regulation' (Bird & Bird, April 2023) https://iapp.org/resources/article/bird-bird-guide-to-the-general-data-protection-regulation/ accessed 21 October 2024, 10:17

[144] European Data Protection Board, 'Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation' (4 June 2019). https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf accessed 21 October 2024, 10:19

[145] 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 L119/1, art 28. https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed 21 October 2024, 10:20

cover the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. They also often include provisions related to data security, breach notification, and the exercise of data subject rights. For example, Salesforce provides a comprehensive data processing addendum that customers can incorporate into their agreements, ensuring GDPR compliance for data processed through Salesforce services.[146]

The standardization of these agreements by major service providers has helped to streamline GDPR compliance for their customers, although care must be taken to ensure that the agreements are tailored to the specific circumstances of each data processing relationship. The development of data processing agreements has led to increased scrutiny of supply chain relationships, with organizations requiring greater transparency and assurances from their vendors regarding data protection practices. This has helped in generalising the aspect of privacy as an essential factor in business associations and procurement procedures.[147]

4.4.4 Codes of Conduct and Certifications

The GDPR provides for the approved codes of conduct and certifications as the means to prove compliance.[148] While the development of these mechanisms is still in progress, many international corporations are participating in their creation and planning for their adoption. The EU Cloud Code of Conduct, which provides GDPR compliance recommendations for Cloud Service Providers (CSPs), has received endorsement from global giants, including Alibaba Cloud, Google Cloud, IBM, and Oracle.[149] The formulation of codes of conduct and certification mechanisms has been under the cooperation of the industry players, the data protection authorities and the EDPB. Such an approach guarantees that the tools being developed are relevant to business needs and are compliant with the law.[150] The adoption of

[146] Salesforce, 'Data Processing Addendum' (Salesforce, 2024) https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf accessed 21 October 2024, 10:22
[147] Gartner, 'Top Strategic Technology Trends for 2024' (Gartner, October 2023) https://tetrate.io/resource/gartner-top-strategic-technology-trends-for-2024-platform-engineering/#:~:text=2024%3A%20Platform%20Engineering-,Gartner%C2%AE%20Top%20Strategic%20Technology%20Trends%20for%202024%3A%20Platform%20Engineering,streamline%20application%20delivery%20by%202026. accessed 21 October 2024, 10:26
[148] GDPR (n 9) arts 40-43.
[149] EU Cloud Code of Conduct, 'About the EU Cloud Code of Conduct' (SCOPE Europe, 2024) https://eucoc.cloud/en/about/about-eu-cloud-coc/ accessed 21 October 2024, 10:28
[150] European Data Protection Board, 'Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679' (4 June 2019). https://www.edpb.europa.eu/our-work-tools/our-

codes of conduct and certifications is expected to provide organizations with a means of demonstrating their commitment to data protection and potentially streamlining compliance processes. However, it is important to note that these mechanisms do not replace the need for organizations to ensure their compliance with the GDPR's requirements.[151]

4.5 Case Studies of Effective Strategies

To illustrate the practical application of these compliance strategies, this section examines case studies of two international corporations that have implemented comprehensive GDPR compliance programmes.

4.5.1 Case Study: Rolls-Royce

Rolls-Royce, a global leader in power and propulsion systems, has implemented a multi-faceted approach to GDPR compliance, i.e.:

Technical Measures: Rolls-Royce has implemented robust encryption for data at rest and in transit. They've also developed advanced tools for data discovery and classification, helping to identify and protect personal data across their complex global operations. The company has invested in a state-of-the-art Security Operations Centre to monitor and respond to potential data breaches in real-time.[152]

Organisational Measures: Rolls-Royce has followed strict measures of the data privacy governance system with the key officer of privacy and a team of officials. The company provides data protection training for roles in the company whereby employees are trained depending on their responsibilities in the organisation.[153] To enhance privacy culture and compliance, Rolls-Royce has established a network of 'Privacy Champions' across different business units. They act as local privacy advocates, raising awareness, offering best practises on data protection, and as interfaces between their respective units and the central privacy group. This decentralised model enables privacy concerns to be integrated into routine

documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en accessed 21 October 2024, 10:30

[151] Information Commissioner's Office, 'Codes of Conduct and Certification' (ICO, 2024) https://ico.org.uk/for-organisations/advice-and-services/codes-of-conduct/ accessed 21 October 2024, 10:33

[152] Rolls-Royce, 'Annual Report 2023' (Rolls-Royce plc, March 2024) 45. https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/annual-report/2024/2023-annual-report.pdf accessed 21 October 2024, 10:35

[153] Rolls-Royce, 'Data Privacy' (Rolls-Royce plc, 2024) https://www.rolls-royce.com/site-services/data-privacy.aspx accessed 21 October 2024, 10:37

functions while keeping compliance standards uniform throughout the enterprise. The training framework comprises updates on regulatory changes, real-life scenarios, and specific guidance on dealing with sensitive data in engineering and manufacturing environments. This makes sure that privacy is part of the business strategies after being considered in every business stage.

Legal Measures: Rolls-Royce also has extensive data transfer measures by means of their legally recognised Binding Corporate Rules for transferring data within the company. In the presented report, the company has integrated new Standard Contractual Clauses in the data processing agreements, thus meeting existing legal requirements.[154] In order to address the issue of GDPR compliance across all of its operations, Rolls-Royce has established an elaborate vendor management programme. This involves periodic assessments, monitoring of compliance and checklists for all the suppliers who deal with personal data. The programme makes it possible to have a cheque on how the companies and organisations in the supply chain adhere to the data protection standards right from the primary suppliers to sub contractors. This is done continually to ensure that they are able to meet the new and changing regulations that are in the industry as well as new challenges in data protection in the international flying business.

Privacy by Design: The data protection principle has been mainstreamed in the development process at Rolls-Royce, where privacy has been adopted right from the design phase in the development of a new feature, product or service. This privacy by design has proved very important for their services that involve handling large volumes of data such as in condition monitoring, maintenance and engine health prognosis. These services gather and analyse large volumes of operational data to forecast when maintenance is needed and how the engine could be optimised; thus, data protection is critical.[155] It also has a privacy policy for its products from the conceptual stage to the development, utilisation and evaluation phase. It also minimises the risks of noncompliance with data protection regulations while preserving the technological advancement that is crucial for complex engineering solutions.

Rolls-Royce's approach demonstrates how technical, organisational, and legal measures can be integrated into a comprehensive GDPR compliance strategy. Their focus on privacy by design

---

[154] Information Commissioner's Office, 'Guide to Binding Corporate Rules' (ICO, 19 December 2023) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/guide-to-binding-corporate-rules/ accessed 21 October 2024, 10:40

[155] Rolls-Royce, 'Digital Innovation' (Rolls-Royce plc, 2024) https://www.rolls-royce.com/innovation/digital.aspx accessed 21 October 2024, 10:44

in product development showcases how data protection can be aligned with innovation in a high-tech manufacturing context.

4.5.2 Case Study: GlaxoSmithKline (GSK)

GSK, a global pharmaceutical company, has implemented a global data privacy programme to ensure GDPR compliance across its diverse operations:

Technical Measures: GSK has developed a centralised consent management platform, allowing for consistent management of data subject consents across its various business units and clinical trials. They have also applied high-level anonymisation and pseudonymisation solutions for research data while addressing the fundamental conflict between privacy and research.[156]

Organisational Measures: GSK has established Data Privacy Officers in all its operations, managed by a Data Privacy Centre of Excellence. They have also put in place roll-based privacy training for employees with a special focus on those engaged in clinical research and pharmacovigilance. The company has also established privacy impact screenings at the start of all personal data projects.[157]

Legal Measures: Binding Corporate Rules for controller and processor activities have been approved at GSK and offer a comprehensive set of rules for intra-Company transfers. They have also developed standardised data-sharing agreements for collaborations with academic institutions and other pharmaceutical companies, ensuring GDPR compliance in complex research partnerships.[158]

Data Protection Impact Assessments: GSK has integrated DPIAs into its project management processes, ensuring that data protection risks are assessed and mitigated early in the development of new products, services, or research initiatives. This has been particularly

[156] GlaxoSmithKline, 'Annual Report 2023' (GSK plc, February 2024) 62. https://www.gsk.com/media/11007/annual-report-2023.pdf accessed 21 October 2024, 10:45
[157] GlaxoSmithKline, 'Privacy Centre' (GSK plc, 2024) https://privacy.gsk.com/en-us/privacy-notice/ accessed 21 October 2024, 10:48
[158] European Data Protection Board, 'Register for Binding Corporate Rules' (EDPB, 2024) https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en accessed 21 October 2024, 10:50

important in their development of digital health solutions and personalised medicine approaches.[159]

GSK's approach highlights the importance of integrating data protection considerations into core business processes and establishing a global privacy governance structure. Their strategy demonstrates how GDPR compliance can be achieved in a highly regulated industry that relies heavily on personal data processing for both commercial and research purposes.

These case studies illustrate how large, complex organisations can implement comprehensive GDPR compliance strategies that address technical, organisational, and legal requirements. Both Rolls-Royce and GSK have demonstrated a commitment to embedding data protection principles into their core business operations, reflecting the increasing importance of privacy as a corporate value and competitive differentiator.

4.6 Conclusion

International business to comply with the GDPR use a number of strategies that are diverse and elaborate, as is the regulation in question. Technical safeguards offer essential support for data protection, and organisational measures guarantee the performance of these technologies; legal safeguards offer the contractual and procedural basis for lawful data processing and transfer. The examples of Salesforce and Siemens show that the GDPR compliance programmes use these measures in unison. They also stress the need for customising compliance approaches in relation to the context of the organisation in question, including the kind of industry, the kinds of data collected, and the geographical reach of business operations. With such changes in the regulatory environment and future judicial decisions as *Schrems II,* global companies need to adapt to changes in their approaches. Engagement in continuous surveillance of changes in the regulatory landscape, periodic review of existing compliance strategies and making privacy a corporate ethos shall be very vital in ensuring compliance with GDPR as the environment changes.

Chapter 5: Challenges in Maintaining GDPR Compliance Across Jurisdictions

5.1 Introduction

[159] GlaxoSmithKline, 'Digital Health and Data Science' (GSK plc, 2024) https://www.gsk.com/en-gb/ accessed 21 October 2024, 10:52

The European Union's General Data Protection Regulation has changed data protection laws worldwide, especially for global organisations. As a relatively new legal initiative for European Union data protection, it poses challenges to organisations operating in multiple legal environments. This chapter focuses on how international firms manage cross-border compliance challenges, legal requirements, enforcement, operations, and conflicts with European Union data localisation laws.

5.2 Varying Legal Standards in Different Countries

5.2.1 Divergent Approaches to Data Protection

Laws concerning data protection differ around the world and regions implement different policies. Compared to GDPR, the main reference for comparison is the California Consumer Privacy Act (CCPA), which is different in terms of scope and responsibilities.[160]

Different standards create challenges for multinational organisations. Beyond understanding various legal systems, they must implement data protection programmes meeting the most stringent jurisdictional requirements while maintaining standardised global processes.

5.2.2 Adequacy Decisions and International Data Transfers

The GDPR regime presents compliance difficulties through the adequacy decision mechanism, in particular in regard to international data transfers. Since the European Commission adequacy status is only granted to a limited number of countries, organisations are forced to lean on SCCs and BCRs when transferring data to non-adequate nations.[161] The *Schrems II* decision has added to this by voiding the EU-US Privacy Shield and adding new conditions to the usage of SCCs. Organisations have to carry out a legal analysis of the third-country laws and apply additional measures that drastically affect the EU-US data transfers and compel multinational corporations to redesign the data transfer processes.[162]

---

[160] *California Consumer Privacy Act of 2018*, Cal. Civ. Code § 1798.100 et seq. (2018). https://cppa.ca.gov/regulations/pdf/cppa_act.pdf accessed 21 October 2024, 10:54

[161] European Commission, 'Adequacy decisions' (European Commission) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed 21 October 2024, 10:57

[162] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311 accessed 21 October 2024, 10:59

5.2.3 Evolving Legal Landscape

The legal framework for data protection is still rapidly changing as new countries adopt and amend their data protection laws. The LGPD set up in Brazil in 2020 is an addition to the current frameworks with requirements that are quite comparable to those in GDPR. This constant evolution means that multinational organisations need to be always alert to legal changes in each jurisdiction and modify their compliance programmes accordingly. The challenges that organisations face include the need to balance a growing array of often interrelated and sometimes incompatible standards while at the same time ensuring that their data protection processes are robust.[163]

5.3 Enforcement Practices Across Jurisdictions

5.3.1 Inconsistent Interpretation and Application

Although the GDPR sought to promote harmonisation of enforcement across the EU, there are still considerable differences in how the Data Protection Authorities of the member states implement the regulation. This inconsistency is particularly felt by MNCs that have operations in more than one EU member state. While the GDPR's 'one-stop-shop' mechanism was designed to streamline enforcement for cross-border processing by establishing a lead supervisory authority, its practical implementation has proven challenging. Substantial complexity and delay emerge when the organisations are trying to identify the lead authority and coordinate the enforcement actions if multiple DPAs are implicated.[164]

5.3.2 Varying Enforcement Priorities and Resources

The fact that different DPAs may have different enforcement priorities and resource endowments may mean that scrutiny for enforcement action against firms in different jurisdictions may be quite dissimilar. This is true because some DPAs have been more active in fine and enforcement notices than others, which have assumed the advisory role.[165] This

---

[163] Lei Geral de Proteção de Dados Pessoais (LGPD), Lei No. 13,709/2018 (2018). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm accessed 21 October 2024, 11:04

[164] European Data Protection Board, 'Guidelines 02/2022 on the application of Article 60 GDPR' (14 March 2022). https://www.edpb.europa.eu/system/files/2022-03/guidelines_202202_on_the_application_of_article_60_gdpr_en.pdf accessed 21 October 2024, 11:05

[165] DLA Piper, 'DLA Piper GDPR fines and data breach survey: January 2024' (DLA Piper, January 2024). https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024 accessed 21 October 2024, 11:07

variation in enforcement practises increases the compliance risk for MNCs and may complicate the process of determining resource allocations. While some jurisdictions may force organisations to adhere strictly to the GDPR rules, others hardly pay any attention to the compliance hence no consistent approach on the global platform.

5.3.3 Extraterritorial Enforcement Challenges

The extraterritoriality of the GDPR concerns the issue of how the regulation will be enforced against organisations that operate outside the EU. Although the regulation gives provisions for measures, for example, the EU representatives, the enforcement against the non-EU actors can still be an issue.[166] This ambiguity of extraterritorial enforcement often results in diverse compliance measures by organisations depending on their perceived enforcement risk, and thus an unequal competition ground in the global market can be the result.

5.4 Operational Complexities for Multinational Corporations

Maintaining GDPR compliance across jurisdictions introduces significant operational complexities for multinational corporations.

5.4.1 Data Mapping and Management

One of the main operational challenges organisations face is maintaining accurate, current data flow maps across global operations. The GDPR requires comprehensive documentation of processing activities and data protection impact assessments, demanding a thorough understanding of personal data movement within and beyond organisational boundaries.[167] This challenge becomes more complicated with advanced IT structure environments from cloud services, distributed data base systems, third-party data sharing, and integration with old systems.

The complexity of data management increases with geographically dispersed storage locations and real-time synchronisation across different countries. Organisations must monitor data

[166] Dan Jerker B. Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stanford Journal of International Law 53. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/stanit50&section=6 accessed 21 October 2024, 11:09

[167] Information Commissioner's Office, 'Documentation' (ICO) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/ accessed 21 October 2024, 11:10

flows through complex networks while ensuring compliance with varying jurisdictional requirements. This calls for complex data mapping solutions, cheques on the data maps, and staff to manage it all. These maps are dynamic in nature and may need to be updated frequently especially where there is installation of new systems or creation of new business relationships.

5.4.2 Implementing Consistent Policies and Procedures

The issue of the policies on the protection of data with multinational operations has been found to pose several complexities in harmonisation. Despite the General Data Protection Regulation providing core values, its enforcement raises numerous questions at the local legal level, culture, and organisational climate. One of the peculiarities and yet another critical issue here is how to obtain the right balance between global standardisation and regional compliance. This complexity is, however, usually felt especially in employment data processing, where national legislation on labour usually dictates certain guidelines and regulations. Such variations affect multiple operational aspects, including personnel record management, data retention protocols, and cross-border transfer mechanisms.

Some jurisdictions impose distinct retention periods for personnel records, enhanced protection measures for employee data, or restrictions on cross-border data transfers. These regulatory variations affect recruitment procedures, performance evaluations, workplace monitoring, and benefits administration. Successful implementation requires alignment with both GDPR principles and local regulations, supported by robust governance structures and regular compliance monitoring.[168]

5.4.3 Training and Awareness

A major operational concern for companies is to guarantee that all employees in the jurisdictions of the company are aware of and adhere to the GDPR. This includes not only the university's initial training, but also periodic awareness programmes with exposure to new interpretations and practises of enforcement. The challenge is magnified in organisations with diverse workforces spread across multiple countries, where language barriers and cultural differences may impact the effectiveness of training programs.

[168] 'GDPR conundrums: Data transfer' (IAPP, 9 June 2016) https://iapp.org/news/a/gdpr-conundrums-data-transfer accessed 21 October 2024, 11:12

5.4.4 Managing Data Subject Rights

The GDPR gives data subjects the following rights, which include the right to access, right to data rectification, right to erasure and right to data portability. Those responsibilities across the operation of these rights are inherently difficult to manage, especially when nurturing data residing on various systems and regions.[169] Organisations need to realise the best ways of identifying the data subjects, finding the data and responding within the set time. Most of these processes entail cross-departmental workflow synchronisation, good technological support, and staff education.

The level of difficulty rises even higher when one considers the possibility of clashes of the GDPR with laws in various parts of the world. For instance, data retention laws in one country may be infringing on GDPR erasure laws. Furthermore, organisations need to keep records of all the processes that are followed when handling requests in order to support compliance. The systems that are used for response management must be compatible with other tools used for data management; the security and privacy of the information must be maintained all the time. Audits also keep the process routine and allow for the assessment of changes required to rights management processes.

5.5 Conflicts Between GDPR and Non-EU Data Localisation Laws

5.5.1 Data Localisation Requirements

Many countries have introduced or are considering laws that require certain types of data to be stored within their national borders. For example, Russia's data localisation law requires that the personal data of Russian citizens be stored on servers physically located within Russia.[170] Similarly, China's Cybersecurity Law imposes data localisation requirements for certain types of data.[171]

---

[169] European Data Protection Board, 'Guidelines 01/2022 on data subject rights - Right of access' (18 January 2022). https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf accessed 21 October 2024, 11:14

[170] Federal Law No. 242-FZ, On Amendments to Certain Legislative Acts of the Russian Federation with Regard to Specifying the Procedure for the Processing of Personal Data in Information and Telecommunication Networks (2014). https://wilmap.stanford.edu/entries/federal-law-no-242-fz accessed 21 October 2024, 11:15

[171] Cybersecurity Law of the People's Republic of China (2016). https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3 accessed 21 October 2024, 11:17

These requirements can conflict with the GDPR's provisions on international data transfers, creating a dilemma for multinational corporations that need to comply with both sets of laws.

5.5.2 Conflicts with GDPR Principles

Data localisation laws are likely to cause tension with generic GDPR principles such as the principles of data minimisation and purposes limitation. If organisations store data in different jurisdictions in order to meet local legal requirements, this could lead to the creation of unnecessary obfuscating copies of personal data and hence expose the data to undue risk of leakages and unauthorised access.

5.5.3 Impact on Global Data Flows

The proliferation of data localisation laws poses a significant challenge to the free flow of data that many multinational corporations rely on for their global operations. Ensuring compliance with these laws alongside GDPR may pose some significant technical challenges that may result in higher costs and lower operations efficiency.[172]

5.5.4 Reconciling Conflicting Legal Obligations

International business organisations face a dilemma of legal compliance at times. For example, the data subject access rights under the GDPR are likely to be inconsistent with data localisation laws that prohibit data export across borders. Satisfying these often-competing demands is a complex legal exercise that usually presents choices between the preferable and the permissible.

5.6 Conclusion

The general management of GDPR across different jurisdictions is a complex issue for multinational organisations. The general legal requirements across the countries are not uniform, enforcement is patchy, the operations are intricate, and data localisation laws pose challenges to organisations. The management of these challenges calls for multisectoral strategies that aim at a legal perspective, technological intervention, and organisational strategies. Today, legal compliance is a dynamic process that requires corporate compliance programmes to be adaptable in response to changing laws and the methods of enforcement by

[172] Anupam Chander and Uyên P Lê, 'Data Nationalism' (2014) 64 Emory LJ 677 https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/emlj64&section=32 accessed 21 October 2024, 11:20

different countries. Ensuring GDPR compliance across jurisdictions will remain a significant challenge for global businesses as the international legal framework for data protection continues to evolve. Addressing this challenge requires vigilant attention, adaptability, and the ongoing integration of data protection principles into core business processes.

Chapter 6: Implications of the Schrems II Decision on International Data Flows

6.1 Introduction

The CJEU judgement in *Data Protection Commissioner v Facebook Ireland Limited*, Maximillian Schrems (commonly known as Schrems II), has brought significant consequences for international data transfers, especially transfers of EU personal data to third countries.[173] Thus, this chapter is centred on the *Schrems II* judgement, the consequences of the judgement to the EU-US data transfers and other countries apart from the US, corporate response to the judgement and various ways of addressing problems arising from the judgement.

6.2 Analysis of the Schrems II Judgment

6.2.1 Background and Key Issues

The main case of this analysis, the Schrems II case, stemmed from the complaint that Max Schrems filed against Facebook Ireland for transferring his data to the company Facebook Inc. in the United States. This landmark case fundamentally challenged two primary mechanisms for international data transfers: The two mechanisms include the EU-US Privacy Shield and the Standard Contractual Clauses or SCCs. Schrems further challenged that the surveillance laws in the US did not afford sufficient protection to the EU citizen's personal data due to a conflict of sovereignty interests between security and privacy.[174]

The case gave rise to important questions regarding the adequacy of protection of personal data in third countries and the efficiency of available transfer tools. It especially scrutinised whether providing almost all branches of US law enforcement, as well as the national security agencies, the very broad access to personal data complied with the EU data protection standards. It was

[173] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311 accessed 21 October 2024, 11:25
[174] ibid, paras 51-68.

an opportunity to understand the interaction of trade in personal data, national security, and basic human rights in the context of advancing digital society

6.2.2 Main Findings of the Court

The CJEU's judgment, delivered on 16 July 2020, contained several key findings:

1. Invalidation of the EU-US Privacy Shield: The Court declared the EU-US Privacy Shield Decision invalid, finding that it did not provide an adequate level of protection for personal data transferred to the United States.[175]
2. Validity of Standard Contractual Clauses: The Court upheld the validity of SCCs as a transfer mechanism in principle. However, it emphasized that the use of SCCs does not absolve data exporters and importers from ensuring that the level of protection required by EU law is respected in the third country.[176]
3. Obligation to Assess Third Country Laws: The Court held that data exporters (in collaboration with data importers) must verify, on a case-by-case basis, whether the law of the third country ensures adequate protection for personal data transferred under SCCs.[177]
4. Suspension of Transfers: If the level of protection cannot be ensured, data exporters are obliged to suspend the transfer of personal data and/or terminate the contract with the data importer.[178]

6.2.3 Legal Reasoning

The Court's decision was primarily based on its assessment of US surveillance laws and practices. It found that the surveillance programmes based on Section 702 of the FISA and Executive Order 12333 did not provide limitations and safeguards comparable to those required under EU law, particularly in light of the principle of proportionality.[179] Furthermore, the Court found that the Ombudsperson mechanism introduced by the Privacy Shield did not provide

[175] ibid, para 201.
[176] ibid, para 134
[177] ibid, para 142.
[178] ibid, para 135.
[179] ibid, paras 168-185.

data subjects with a cause of action before a body offering guarantees substantially equivalent to those required by EU law.[180]

6.3 Impact on EU-US Data Transfers

The *Schrems II* decision has had significant implications for EU-US data transfers, creating legal uncertainty and operational challenges for businesses.

6.3.1 Invalidation of the Privacy Shield

The recent declaration of the Court of Justice of the European Union (CJEU) that called into question the lawfulness of the EU-US Privacy Shield framework disrupted thousands of organisations from the moment it was made. More than 5,000 American organisations used this structure as the sole legal basis for moving personal data between the EU and the US. The invalidation completely eradicated their legal ground for processing data transfers in the middle of the night, and these organisations started looking for new ways to seek compliance or else they would be in violation of GDPR. As most organisations laboured to align themselves to the new legal requirements for processing data across the Atlantic, many struggled with operational issues.[181]

6.3.2 Challenges in Using SCCs for EU-US Transfers

The Court upheld Standard Contractual Clauses as valid but imposed significant new requirements that complicated their use for EU-US transfers. Organisations are now required to undertake specific evaluations regarding the extent to which US law offers sufficient protection to transferred data, with reference to the surveillance legislation and capabilities in the United States. This evaluation has been particularly difficult since the Court has directly condemned US surveillance laws and programmes. It has become increasingly difficult for many organisations to continue to rely on SCCs to transfer data to the US because of the basic threats posed by the surveillance capacity of the US government and the lack of adequate remedy for any EU citizen.[182]

---

[180] ibid, paras 186-197.
[181] International Association of Privacy Professionals, 'The Schrems II Decision: EU-US Data Transfers in Question' (IAPP, 16 July 2020). https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question accessed 21 October 2024, 11:45
[182] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (10 November 2020).

6.3.3 Need for Supplementary Measures

In the wake of the Schrems II judgement, the European Data Protection Board provided extensive guidance on additional measures organisations should put in place in connexion with SCCs. Such measures include but are not limited to, technical protection measures as follows: encryption and pseudonymisation measures and adequate data minimisation policies. Organisations also need to put down organisational protections and upgrade contractual terms. Nevertheless, it has been a challenge to implement these add-on measures effectively across all EU-US data transfers for many organisations, especially with today's intricate data flows and the continual need for business operations.[183]

6.4 Relevance for Data Transfers from the EU to Non-US Countries

While the *Schrems II* decision focused on EU-US transfers, its implications extend to data transfers to all third countries.

6.4.1 Case-by-Case Assessment Requirement

The judgement made a ruling that organisations ought to assess the laws of each of the third countries that are involved in data transfers apart from the US. This assessment must determine if the legal regime of the recipient country offers a sufficient level of data protection. Businesses receiving data across borders are now in for the challenge of trying to understand different legal systems and data protection regimes. This requirement has put tremendous pressure on multinational organisations that often transfer data across borders.[184]

6.4.2 Focus on Government Access to Data

The *Schrems II* decision raised questions about government surveillance authorities in third countries. The Court's assessment of government access to people's personal data is most pertinent to nations with vast surveillance programmes. This scrutiny has created much concern about the transfer of data to countries such as China, Russian and India due to the authorities who have unrestricted access to personal data. It means that organisations today have to

---

https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en accessed 21 October 2024, 11:50

[183] ibid.

[184] Christopher Kuner, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (2020) European Law Blog. http://www.kuner.com/my-blog-entries.html accessed 21 October 2024, 11:57

consider the surveillance laws and practices in these countries when considering the possibility of data transfer.[185]

6.4.3 Impact on Adequacy Decisions

This judgement has profound consequences for the European Commission's adequacy decisions. The Commission has to apply higher criteria in the evaluation of third countries' data protection now. This increased attention applies to current adequacy decisions as well as to decisions that will be made in the future. Member states that currently enjoy adequacy decisions may find it hard to sustain this status, which could lead to a disruption of the data flows. Some of the key findings highlighted above suggest that the Commission's future adequacy assessments will probably need more scrutiny of surveillance laws and remedies in third states.[186]

6.5 Corporate Responses to Schrems II

The reactions of organisations to the *Schrems II* decision have been in different and diverse ways due to the complexity of the problems that arise with the need to transfer data.

6.5.1 Re-evaluation of Data Flows

Most organisations have carried out assessments of their international data transfers, covering the kind of data that is transferred and the reason for the transfer. As a result of this assessment, many organisations have been forced to rationalise their data flows, and some have decided to move certain data processing activities within the EU to avoid complications. This data localization approach forms a new model that is a departure from how organisations manage their data operations across borders.[187]

---

[185] 'The Definitive Guide to Schrems II' (OneTrust DataGuidance, 22 November 2022) https://www.dataguidance.com/resource/definitive-guide-schrems-ii accessed 21 October 2024, 12:10

[186] European Commission, 'Adequacy decisions' (European Commission) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed 21 October 2024, 12:15

[187] 'The impact of the 'Schrems II' case on personal data' (KPMG Law, 2020) https://kpmglaw.be/news/posts/2020/august/the-impact-of-the-schrems-ii-case-on-personal-data/ accessed 21 October 2024, 12:18

6.5.2 Implementation of Supplementary Measures

The organisations who have continued to use Standard Contractual Clauses have put in place adequate supplementary measures relying on the EDPB guidance, including the utilisation of greatly improved encryption measures for data both in transit and at rest, advanced techniques in the anonymization of personal identifiers from other data components and strict access control measures using multi-factor authentication and permissioned access. These broad technical measures help safeguard transferred data from access by governments in recipient countries while establishing practical mechanisms for demonstrating compliance based on the technical audit trails and frequent security cheques.[188]

6.5.3 Exploration of Alternative Transfer Mechanisms

Following the *Schrems II*, organisations have sought other options for intra-group transfers of data: Binding Corporate Rules is one of them. BCRs provide a framework for Multinational undertakings to transfer data within their corporate group while maintaining the same level of protection for data. The approval process for Binding Corporate Rules requires extensive documentation and review by multiple supervisory authorities, typically taking 12-18 months or longer to complete. This lengthy and resource-intensive approval timeline has rendered BCRs ineffective as an immediate fix for those organisations that need to establish new, GDPR-compliant data transfer mechanisms swiftly in the aftermath of the *Schrems II* decision.[189]

6.5.4 Contractual and Organizational Changes

In response to Schrems II requirements, companies have redesigned their data processing contracts and internal regulations significantly. These changes now include additional text describing how the company would process government access requests, strict rules on notification when such requests are received, and additional transparency requirements for data

[188] Rob van Eijk and Gabriela Zanfir-Fortuna, 'Schrems II: Article 49 GDPR Derogations May Not Be So Narrow and Restrictive After All?' (Future of Privacy Forum, 4 February 2021) https://fpf.org/blog/schrems-ii-article-49-gdpr-derogations-may-not-be-so-narrow-and-restrictive-after-all/ accessed 21 October 2024, 12:25
[189] Bird & Bird, 'Guide to the General Data Protection Regulation' (Bird & Bird, April 2023). https://www.twobirds.com/-/media/new-website-content/pdfs/capabilities/privacy-and-data-protection/bird-and-bird-gdpr-guide.pdf accessed 21 October 2024, 12:30

transfers. Transfers have also been reinforced documentation pertaining to the transfer impact assessment and additional measures to show compliance with GDPR.[190]

6.6 Proposed Solutions

Various solutions have been proposed or are in development to address the challenges created by the *Schrems II* decision.

6.6.1 New EU-US Data Privacy Framework

In March 2022, the EU and the US came up with the new Trans-Atlantic Data Privacy Framework to replace the defunct Privacy Shield deal. This framework brings major changes to respond to the main issues raised by *Schrems II*, such as restrictions on the surveillance capabilities of US intelligence and their access to data of EU persons. A critical component is the creation of a new redress mechanism for EU citizens to challenge US surveillance practices, aiming to provide the "effective remedy" that the Court found lacking in previous arrangements.[191]

6.6.2 Updated Standard Contractual Clauses

The European Commission's updated Standard Contractual Clauses (SCCs) directly address the *Schrems II* requirements through enhanced obligations for both data exporters and importers. These new SCCs include specific provisions for reporting government access requests, substantial evaluation of third countries' legislation impacting data protection, and precise measures for handling government surveillance requests. The clauses also enhance the need to document compliance and, where necessary, introducing additional measures to enhance data protection.[192]

---

[190] DLA Piper, 'DLA Piper GDPR fines and data breach survey: January 2024' (DLA Piper, January 2024) https://blogs.dlapiper.com/advocatus/files/2024/01/DLA-Piper-GDPR-fines-and-Data-Breach-Report-2024.pdf accessed 21 October 2024, 12:37

[191] European Commission, 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework' (European Commission, 25 March 2022). https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/united-states-and-european-commission-joint-statement-on-trans-atlantic-data-privacy-framework/#:~:text=Under%20the%20Trans%2DAtlantic%20Data,with%20binding%20authority%20to%20direct accessed 21 October 2024, 12:45

[192] 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 L199/31. https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj accessed 21 October 2024, 12:55

6.6.3 Code of Conduct for Cloud Service Providers

The EU Cloud Code of Conduct has undergone a major revision in order to include the *Schrems II* requirements for cloud service providers. The Code now has comprehensive information on international data transfers in cloud solutions and concrete measures regarding GDPR. This framework aids the cloud service providers to meet the demands of data protection requirements by the use of standardised means of data transfer, security measures and transparency.[193]

6.6.4 Technical Solutions

The *Schrems II* decision has led organisations to develop complex technical measures to safeguard data transfers. Modern encryption techniques now encompass current encryption standards for data in storage and while in transit. Confidential computing technologies solve the hardware layer by performing computation in trusted execution environments, whereas PETs, such as homomorphic encryption, facilitate data analysis without revealing the raw personal data. These technical means together generate several levels of protection that make personal data virtually non-apprehensible to third parties and state surveillance.[194]

6.7 Conclusion

The *Schrems II* decision has substantially changed the legal framework governing international data transfers thus posing multiple challenges to organisations. While the decision's immediate focus was on EU-US transfers, its implications extend to data flows to all third countries. Organizations have had to reassess and often restructure their data transfer practices, implementing new legal, technical, and organizational measures to ensure compliance. The new EU-US framework, as well as the new SCCs, present ways forward for transfers of data across borders. The legal and practical issues that arise from *Schrems II* thus mean that organisations need to be agile and adaptive. With the world changing on data protection laws, the principles set in *Schrems II* will be key to defining the future of the cross-border data transfer.

---

[193] EU Cloud Code of Conduct, 'About the EU Cloud Code of Conduct' (SCOPE Europe, 2024) https://eucoc.cloud/en/about/about-eu-cloud-coc/ accessed 21 October 2024, 12:59

[194] 'What is confidential computing?' (IBM, 4 June 2024) https://www.ibm.com/topics/confidential-computing accessed 21 October 2024, 13:01

Chapter 7: Findings and Discussion

7.1 Introduction

This chapter discusses the research questions and hypotheses which have been presented in the first chapter. Through analysis of empirical data and case studies, this research examines how multinational organizations can benefit from good policies and practices for data protection. These policies and practices contribute to enhanced operational efficiency in organizations. The research also identifies the practical challenges that multinational organisations face when implementing GDPR. The study also responds to the research questions based on the hypothesis that operational challenges for companies that implement the GDPR continue to be challenging, and that the Schrems II decision further complicates international data transfers. It concentrates on how *Schrems II* decision affects international data transfers in companies within and outside EU. As stated in the introduction, this chapter focuses on analysing how companies have changed their approach to data management, employed new protection measures and adjusted their business structures to address these emergent compliance needs.

7.2 Synthesis of Research Findings

7.2.1 GDPR Compliance Strategies in International Corporations

This research has outlined several strategies adopted by global organisations towards GDPR compliance. These strategies can be categorised into technical, organisational and legal approaches and are frequently combined to provide a comprehensive compliance programme. Technical measures form the foundation of many compliance strategies. Encryption and pseudonymization have emerged as key technologies employed by international corporations to protect personal data during cross-border transfers. For instance, Microsoft's implementation of encryption for data in transit between users and data centres, as well as for data moving between data centres, exemplifies the adoption of robust technical measures.[195] The use of data discovery and classification tools, as offered by services like Amazon Macie, has become crucial for implementing data minimization and purpose limitation principles effectively across global operations.[196]

[195] Microsoft, 'Encryption in the Microsoft Cloud' (Microsoft Trust Center, 2024) https://learn.microsoft.com/en-us/purview/office-365-encryption-in-the-microsoft-cloud-overview accessed 21 October 2024, 13:08
[196] 'AWS Cloud Security' (Amazon Web Services) https://aws.amazon.com/security/ accessed 21 October 2024, 13:10

Organizational measures have proven equally important in ensuring GDPR compliance. The appointment of Data Protection Officers (DPOs) has become standard practice among international corporations, even when not strictly required by the GDPR. Volkswagen Group's establishment of a network of DPOs across its global operations, coordinated by a Group Data Protection Officer, demonstrates how large multinational corporations are implementing centralized yet locally responsive data protection strategies.[197] Comprehensive employee training programs, such as those implemented by Accenture, have been identified as crucial for creating a culture of data protection throughout organizations.[198]

Legal measures, particularly the use of Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), have been widely adopted to provide a legal basis for international data transfers. However, the research has shown that in the wake of the *Schrems II* decision, these mechanisms are increasingly being supplemented with additional safeguards to ensure their effectiveness.[199]

7.2.2 Challenges in Maintaining GDPR Compliance Across Jurisdictions

The research has identified several key challenges faced by internationally operating corporations in maintaining GDPR compliance across different jurisdictions. These challenges stem from varying legal standards, inconsistent enforcement practices, operational complexities, and conflicts between the GDPR and non-EU data localization laws. International organisations face challenges due to varying data protection standards across countries. The GDPR sets stringent requirements, yet national laws differ in their approach. For example, the legislation similar to the GDPR, which is in force in the United States, is called the California Consumer Privacy Act (CCPA), but even in terms of covering definitions and some specific provisions, they are not the same.[200] Corporations must adhere to varying compliance standards across countries, often adopting the highest to avoid complications.

---

[197] 'Privacy policy' (Volkswagen Group) https://www.volkswagen-group.com/en/privacy-policy-15677 accessed 21 October 2024, 13:12

[198] 'Keeping our clients' data safe' (Accenture) https://www.accenture.com/us-en/case-studies/about/keeping-accenture-client-data-protected accessed 21 October 2024, 13:16

[199] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (10 November 2020). https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en accessed 21 October 2024, 13:18

[200] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (2018). https://cppa.ca.gov/regulations/pdf/cppa_act.pdf accessed 21 October 2024, 13:29

Despite GDPR's aim to standardize data protection enforcement across the EU, this research reveals ongoing disparities in how national Data Protection Authorities (DPAs) implement the regulation. This variation in enforcement practices from one region to another continues to challenge the uniform application of data protection standards. This inconsistency can lead to uncertainty for multinational corporations, especially when operating across multiple EU member states.[201] Operational complexities, particularly in maintaining accurate data maps and implementing consistent policies and procedures across diverse global operations, have been identified as a major challenge. The GDPR's requirements for documenting processing activities and conducting data protection impact assessments necessitate a comprehensive understanding of how personal data moves within and outside the organization, a task that is complicated by the complexity of modern IT infrastructures.[202]

Conflicts between the GDPR and non-EU data localization laws present another significant challenge. Many countries have introduced or are considering laws that require certain types of data to be stored within their national borders. For example, Russia's data localization law requires that the personal data of Russian citizens be stored on servers physically located within Russia.[203] These requirements can conflict with the GDPR's provisions on international data transfers, creating a dilemma for multinational corporations that need to comply with both sets of laws.

7.2.3 Implications of the Schrems II Decision on International Data Flow Practices

The study has shown that the *Schrems II* decision has had a massive impact on international data transfers, especially on transfers to third countries of personal data from the EU. The annulment of the EU-US Privacy Shield gave many businesses no valid legal ground for transferring personal data from the EU to the USA, thereby requiring them to find new ways to perform the transfers.[204] The Court of Justice of the European Union (CJEU) upheld the

---

[201] LA Piper, 'DLA Piper GDPR fines and data breach survey: January 2024' (DLA Piper, January 2024). https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024 accessed 21 October 2024, 13:31

[202] Information Commissioner's Office, 'Documentation' (ICO, 2024) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/ accessed 21 October 2024, 13:32

[203] Federal Law No. 242-FZ, On Amendments to Certain Legislative Acts of the Russian Federation with Regard to Specifying the Procedure for the Processing of Personal Data in Information and Telecommunication Networks (2014). https://wilmap.stanford.edu/entries/federal-law-no-242-fz accessed 21 October 2024, 13:36

[204] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311 accessed 21 October 2024, 13:38

validity of Standard Contractual Clauses (SCCs) in principle but added requirements complicating their use for EU-US transfers. Data exporters must now assess whether third-country laws provide sufficient protection under SCCs, a challenge given the Court's rejection of US surveillance law adequacy.[205]

The implications of the *Schrems II* decision go beyond EU-US transfers. It is important to note that the Court's consideration of the general applicability to and the assessment of the impact of third-country laws accords with all international data transfers not limited to the US. This has created a significant burden for organizations transferring data to multiple countries, as they must assess the legal landscape in each destination country.[206] In response to these challenges, many international corporations have undertaken comprehensive reviews of their international data flows, implemented supplementary measures alongside SCCs, and explored alternative transfer mechanisms such as Binding Corporate Rules (BCRs).[207]

7.3 Evaluation of Hypotheses

The research findings allow for a critical evaluation of the hypotheses proposed at the outset of this study.

7.3.1 Hypothesis 1: Range of GDPR Compliance Strategies

The first hypothesis posited that international corporations adopt a range of strategies to manage GDPR compliance, including technical, organizational, and legal measures. The results of the study confirm this hypothesis. This study has reviewed a wide range of compliance practises adopted by international corporations that include technical solutions like encryption and data discovery tools, organisational solutions such as DPOs and compliance training, and legal solutions like SCCs and BCRs. Microsoft, Volkswagen, and Accenture are

[205] Christopher Kuner, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (2020) European Law Blog. http://www.kuner.com/my-blog-entries.html accessed 21 October 2024, 13:40
[206] Andraya Flor, 'The Impact of Schrems II: Next Steps for U.S. Data Privacy Law' (NDLScholarship) https://scholarship.law.nd.edu/ndlr/vol96/iss5/10/ accessed 21 October 2024, 13:45
[207] 'The impact of the 'Schrems II' case on personal data' (KPMG Law, August 2020) https://kpmglaw.be/news/posts/2020/august/the-impact-of-the-schrems-ii-case-on-personal-data/ accessed 22 October 2024 11:28

examples of organisations that use all these measures in formulating compliance strategies, as shown below.[208]

7.3.2 Hypothesis 2: Key Challenges in GDPR Compliance

The second hypothesis stated that it is seen that the legal requirements of GDPR, the enforcement of laws in different countries and the operational issues are the primary concerns. The research findings will support this hypothesis. In this regard, the study has revealed systematic differences in the legal frameworks of data protection and enforcement across different jurisdictions that have made it challenging for multinational corporations to navigate.[209] Operational complexities, particularly in maintaining accurate data maps and implementing consistent policies across global operations, have emerged as major challenges.[210]

7.3.3 Hypothesis 3: Implications of the Schrems II Decision

The third hypothesis stated that the *Schrems II* decision has significant implications, requiring corporations to reassess and adjust their data transfer mechanisms. The research findings provide strong support for this hypothesis. The invalidation of the EU-US Privacy Shield and the additional requirements imposed on the use of Standard Contractual Clauses (SCCs) have necessitated a fundamental reassessment of international data transfer practices.[211] The study has shown that corporations have had to undertake comprehensive reviews of their data flows, implement supplementary measures alongside SCCs, and explore alternative transfer mechanisms. Furthermore, the implications of the decision extend beyond EU-US transfers,

---

[208] Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide (Springer 2017). https://link.springer.com/content/pdf/10.1007/978-3-319-57959-7.pdf accessed 22 October 2024 11:30

[209] Anupam Chander and Uyên P. Lê, 'Data Nationalism' (2014) 64 Emory Law Journal 677. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/emlj64&section=32 accessed 22 October 2024 11:35

[210] W. Gregory Voss, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29(3) Washington International Law Journal 485. https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1844&context=wilj accessed 22 October 2024 11:37

[211] European Data Protection Board, 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures' (10 November 2020). https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf accessed 22 October 2024 11:43

affecting data flow to all third countries and requiring case-by-case assessments of third-country laws.[212]

7.4 Critical Analysis of GDPR Compliance Strategies and Challenges

The research findings allow for a critical analysis of the GDPR compliance strategies adopted by international corporations and the challenges they face. While the strategies identified demonstrate a concerted effort to address the requirements of the GDPR, they also reveal certain limitations and areas for improvement. The technical measures adopted by corporations, such as encryption and data discovery tools, provide a strong foundation for data protection. However, the rapidly evolving nature of technology and cyber threats necessitates continuous innovation and updating of these measures. Research indicates many corporations have robust measures for data in transit and at rest but less focus on protection during processing, especially in complex distributed computing environments.[213]

Appointing Data Protection Officers and implementing training programs embed data protection principles into corporate cultures. The effectiveness varies based on DPO authority and training quality. The risk of compliance fatigue exists when training initiatives are poorly designed or overly frequent.[214] Standard Contractual Clauses and Binding Corporate Rules provide a legal framework for international data transfers. The *Schrems II* decision highlighted their limitations when used alone. Case-by-case assessments of third-country laws pose challenges, particularly for smaller organizations with limited legal resources.[215]

Global and jurisdictional GDPR compliance demonstrates the conflict between data-free movement and the protection of territorial sovereignty. It is a diverse structure due to the variation in legal norms and the ways that they are implemented, which is augmented by data

---

[212] Christopher Kuner, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (2020) European Law Blog. http://www.kuner.com/my-blog-entries.html accessed 22 October 2024 11:47

[213] European Union Agency for Cybersecurity, 'Data Pseudonymisation: Advanced Techniques and Use Cases' (ENISA, January 2024). https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases accessed 22 October 2024 11:50

[214] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ('DPOs')' (WP 243 rev.01, 5 April 2017). https://ec.europa.eu/newsroom/just/document.cfm?doc_id=44100 accessed 22 October 2024 11:54

[215] European Commission, 'Standard Contractual Clauses (SCC)' (European Commission, 4 June 2021) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en accessed 22 October 2024 11:58

localization rules that can be inconsistent with GDPR transfers.[216] Multi-national organisations are experiencing difficulties in their compliance initiatives, especially as it relates to mapping data and maintaining harmonisation of policies. While acquiring management tools the issue of lack of integration with core business systems might be seen as compliance risks.[217]

7.5 Assessment of Schrems II Implications on International Data Flow Practices

The *Schrems II* judgement has transformed the international data transfer landscape and put into question business models that rely on cross-border data transfers. The annulment of the EU-US Privacy Shield left a legal gap for thousands of organisations conducting business between these regions. Although most organisations have transitioned to SCCs, the further requirements set out in *Schrems II* make this transition difficult. Data exporters are now under immense pressure to assess protection sufficiency in the countries to which the data is transferred, especially concerning governmental monitoring.[218]

The *Schrems II* decision has implications that go beyond the transfers between the EU and the US, and it applies to data transfers to all third countries. Such a broader impact has led to a need for risk analysis of data protection laws and practices for all countries where personal data is transferred. This requirement has been a problem, especially for cloud service providers and other organizations that have networks crossing different geographical boundaries with ever-changing data traffic.[219]

The *Schrems II* decision has also highlighted the tension between data protection requirements and national security interests. The EU Court of Justice's assessment of US surveillance laws impacts how data protection authorities evaluate protection adequacy in countries with

---

[216] Omer Tene and Christopher Wolf, 'Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation' (The Future of Privacy Forum, January 2013) https://fpf.org/wp-content/uploads/2013/01/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20131.pdf accessed 22 October 2024 12:05

[217] Gartner, 'Top Strategic Technology Trends for 2024' (Gartner, October 2023) https://www.gartner.com/en/information-technology/insights/top-technology-trends#:~:text=Here%20are%20the%202024%20top,Sustainable%20Technology accessed 22 October 2024 12:09

[218] European Data Protection Board, 'Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems' (23 July 2020). https://www.edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en accessed 22 October 2024 12:11

[219] Information Commissioner's Office, 'International Data Transfer Agreement and Guidance' (ICO, 2024) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/ accessed 22 October 2024 12:15

extensive surveillance powers.[220] In response, international corporations have adopted risk-based approaches, implemented encryption and kept sensitive data within the EU.[221] While the proposed EU-US Data Privacy Framework addresses Schrems II concerns, its legal sufficiency under EU law remains questionable.[222]

7.6 Conclusion

The outcomes of this research contribute to the understanding of the approaches used by global companies to address GDPR compliance within data transfers, the issues that arise in various jurisdictions, and the effects brought by the Schrems II decision in relation to data transfers. The research work has shown that data protection compliance is a dynamic process in a global environment that requires the use of technical, organisational, and legal solutions. The research has also brought out the realisation that different legal requirements, unequal compliance levels, and competing regulatory frameworks present a major concern. Such challenges are most apparent when international corporations are dealing with data flows across borders.

Schrems II has proven to be a significant turning point in international data transfer practise and has forced a critical reevaluation of other key aspects of transfer mechanisms and data protection, with critical questions left unanswered as to how the remaining interests, such as national security and economic welfare may be balanced with data protection interests. By progressing the international legislation and changing the points demanding the protection of personal data, international companies will need to be flexible in their activity, constantly changing the approach to the legislation and the application of the technologies. It is on these realisations that the findings of this study can be underpinned in order to establish the best ways of dealing with these challenges.

Chapter 8: Conclusion

---

[220] Maja Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core' (2018) 14 European Constitutional Law Review 332. https://doi.org/10.1017/S1574019618000159 accessed 22 October 2024 12:19

[221] Rob van Eijk and Gabriela Zanfir-Fortuna, 'Schrems II: Article 49 GDPR Derogations May Not Be So Narrow and Restrictive After All?' (Future of Privacy Forum, 4 February 2021) https://fpf.org/blog/schrems-ii-article-49-gdpr-derogations-may-not-be-so-narrow-and-restrictive-after-all/ accessed 22 October 2024 12:25

[222] European Commission, 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework' (European Commission, 25 March 2022). https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/united-states-and-european-commission-joint-statement-on-trans-atlantic-data-privacy-framework/#:~:text=Under%20the%20Trans%2DAtlantic%20Data,with%20binding%20authority%20to%20direct accessed 22 October 2024 12:30

8.1 Summary of Key Findings

This thesis has provided an explorative investigation of the approaches adopted by international business organisations and the issues they encounter in regulating the movement of personal data within the context of GDPR compliance. The study has produced several important findings that can be useful for explaining the state of GDPR compliance with regard to cross-border data transfers.

Firstly, the study has established that international corporations use technical, organisational, and legal solutions for GDPR compliance. Encryption and pseudonymization, as well as discovery tools, remain the core of many compliance programmes.[223] These measures are of paramount importance for data transfers to third countries and for the application of principles of data minimization and purposes limitation. Some of the corporate practises that are quite effective in establishing corporate culture towards the protection of data are the appointment of Data Protection Officers (DPOs) and Employee awareness training programmes.[224] Legal measures, particularly the use of Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), provide the necessary framework for lawful international data transfers.[225]

Secondly, the research has established various issues that multinational organisations experience in their quest to adhere to GDPR in various territories. These comprise issues of legal compliance, enforcement disparities, organisation dilemmas, and GDPR incongruity with non-EU data residency laws.[226] The varying legal standards for data protection in different countries create a complex landscape that requires corporations to implement the highest common denominator of data protection standards across their global operations. Inconsistent enforcement practices by different national data protection authorities add another layer of

---

[223] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 2. http://dx.doi.org/10.1007/978-3-319-57959-7 accessed 22 October 2024 12:35

[224] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ('DPOs')' (WP 243 rev.01, 5 April 2017). https://ec.europa.eu/newsroom/just/document.cfm?doc_id=44100 accessed 22 October 2024 12:40

[225] Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18 German Law Journal 881. https://doi.org/10.1017/S2071832200022197 accessed 22 October 2024 12:47

[226] W. Gregory Voss, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29(3) Washington International Law Journal 485. https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1844&context=wilj accessed 22 October 2024 12:50

complexity, making it difficult for corporations to establish a consistent global approach to GDPR compliance.[227]

Thirdly, the study has highlighted the profound implications of the Schrems II decision on international data flow practices. The invalidation of the EU-US Privacy Shield and the additional requirements imposed on the use of SCCs have necessitated a fundamental reassessment of data transfer mechanisms.[228] This decision has not only affected EU-US transfers but has broader implications for data flows to all third countries, requiring case-by-case assessments of third-country laws and the implementation of supplementary measures.[229]

8.2 Reflection on Research Questions and Hypotheses

The research findings provide valuable insights into the research questions posed at the outset of this study:

1. How do internationally operating corporations manage the flow of personal data to ensure compliance with GDPR regulations?

The study has shown that international corporations employ a range of strategies, including robust technical measures like encryption and data discovery tools, organizational measures such as the appointment of DPOs and comprehensive training programs, and legal measures including SCCs and BCRs. These strategies are often implemented in combination to create a comprehensive compliance framework that addresses the complex requirements of the GDPR.[230]

2. What are the key challenges faced by internationally operating corporations in maintaining GDPR compliance across different jurisdictions?

---

[227] DLA Piper, 'DLA Piper GDPR fines and data breach survey: January 2024' (DLA Piper, January 2024). https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024 accessed 22 October 2024 12:50

[228] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311 accessed 22 October 2024 12:53

[229] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (10 November 2020). https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en accessed 22 October 2024 12:55

[230] Lokke Moerel, 'GDPR Conundrums-The Data Protection Officer Requirement' (2016) https://assets.contentstack.io/v3/assets/blt5775cc69c999c255/blt4acf7754cc1e1db6/160719gdprconundrumsdpo.pdf accessed 22 October 2024 12:57

The research has identified several key challenges, including varying legal standards across jurisdictions, inconsistent enforcement practices, operational complexities in maintaining accurate data maps and consistent policies across global operations, and conflicts between the GDPR and non-EU data localization laws. These issues require another sophisticated and flexible approach to compliance that might be suitable for different countries and their legislation that international corporations must face.[231]

3. What are the implications of the Schrems II decision on the international data flow practices of internationally operating corporations?

The Schrems II decision has had far-reaching implications, requiring corporations to reassess and often restructure their data transfer practices. The decision has necessitated more rigorous assessments of third-country laws, the implementation of supplementary measures alongside SCCs, and, in some cases, the exploration of alternative transfer mechanisms or data localization strategies. The implications extend beyond EU-US transfers, affecting data flows to all third countries and requiring a more comprehensive approach to ensuring the adequacy of protection for personal data transferred outside the EU.[232]

Reflecting on the hypotheses proposed at the beginning of the study:

1. International corporations adopt a range of strategies to manage GDPR compliance, including technical, organizational, and legal measures.

The research findings strongly support this hypothesis. The study has identified a diverse array of compliance strategies implemented by international corporations, encompassing technical, organizational, and legal measures. The case studies discussed in the research show how these various measures are integrated to develop complex compliance systems.[233]

---

[231] Anupam Chander and Uyên P Lê, 'Data Nationalism' (2014) 64 Emory LJ 677 https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/emlj64&section=32 accessed 22 October 2024 12:59

[232] Christopher Kuner, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (2020) European Law Blog. http://www.kuner.com/my-blog-entries.html accessed 22 October 2024 13:02

[233] Microsoft, 'Encryption in the Microsoft Cloud' (Microsoft Trust Center, 2024). https://learn.microsoft.com/en-us/purview/office-365-encryption-in-the-microsoft-cloud-overview accessed 22 October 2024 13:05

2. Key challenges include varying legal standards, enforcement practices across jurisdictions, and operational complexities.

This hypothesis is also supported by the results obtained in the course of the research. The research has established fundamental differences in approaches to data protection legislation and compliance, variations in enforcement, as well as practical challenges in achieving uniformity of compliance across different locations. Furthermore, the study has brought out the conflict arising from GDPR and non-EU data localization laws as part of the research hypotheses that were not average in the hypothesis but are important concepts.[234]

3. The Schrems II decision has significant implications, requiring corporations to reassess and adjust their data transfer mechanisms.

The research findings provide strong support for this hypothesis. The invalidation of the EU-US Privacy Shield and the additional requirements imposed on the use of SCCs have indeed necessitated a fundamental reassessment of international data transfer practices. The study has shown that corporations have had to undertake comprehensive reviews of their data flows, implement supplementary measures, and, in some cases, explore alternative transfer mechanisms or data localization strategies.[235]

8.3 Implications for International Corporations and Data Protection Practices

The findings of this study have several important implications for international corporations and data protection practices:

Need for Integrated Compliance Strategies: The research underscores the importance of developing integrated compliance strategies that combine technical, organizational, and legal measures. International corporations need to ensure that these different aspects of compliance work in harmony to create a robust and adaptable data protection framework.[236]

---

[234] Omer Tene and Christopher Wolf, 'Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation' (The Future of Privacy Forum, January 2013) https://fpf.org/wp-content/uploads/2013/01/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20131.pdf accessed 22 October 2024 13:08

[235] 'The impact of the 'Schrems II' case on personal data' (KPMG Law, August 2020) https://kpmglaw.be/news/posts/2020/august/the-impact-of-the-schrems-ii-case-on-personal-data/ accessed 22 October 2024 13:10

[236] Bart Custers and others, *EU Personal Data Protection in Policy and Practice* (T.M.C. Asser Press 2019) 25-30. http://dx.doi.org/10.1007/978-94-6265-282-8 accessed 22 October 2024 13:15

Continuous Adaptation and Assessment: Given the rapidly evolving regulatory landscape and the ongoing challenges posed by varying legal standards and enforcement practices, international corporations must adopt a stance of continuous adaptation and assessment. Subsequently, compliance cheques and balances, data transfer, and risk evaluation periodicals shall be vital to sustaining GDPR compliance across geographical locations.[237]

Enhanced Due Diligence for International Data Transfers: *Schrems II* has left international corporations with no option but to exercise more rigour and apply adequate protection measures to all cross-border transfers. This entails performing elaborate cheques on the third country's laws, putting into writing additional safeguards and being ready to cease the data transfers if adequate protection cannot be afforded.[238]

Investment in Data Protection Expertise: The extent of compliance with the GDPR rules in an international environment requires massive investment in the sphere of data protection specialists. This may involve expanding data protection teams, providing ongoing training and education for employees, and potentially engaging external experts to navigate particularly complex compliance challenges.[239]

Proactive Engagement with Regulators: Given the inconsistencies in enforcement practices across jurisdictions, international corporations may benefit from proactive engagement with data protection authorities. This could involve seeking guidance on complex compliance issues, participating in regulatory consultations, and contributing to the development of codes of conduct or certification mechanisms.[240]

Consideration of Data Localization Strategies: While not mandated by the GDPR, the research suggests that some international corporations are considering data localization strategies to address the challenges of cross-border data transfers. Organizations may need to

---

[237] Gartner, 'Top Strategic Technology Trends for 2024' (Gartner, October 2023). https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2024 accessed 22 October 2024 13:17

[238] European Data Protection Board, 'Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems' (23 July 2020). https://www.edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en accessed 22 October 2024 13:20

[239] 'PECB GDPR Certified Data Protection Officer' (PECB African Training Institute) https://afralt.org/pecb-gdpr-certified-data-protection-officer/ accessed 22 October 2024 13:27

[240] Information Commissioner's Office, 'Codes of Conduct and Certification' (ICO, 2024). https://ico.org.uk/for-organisations/advice-and-services/codes-of-conduct/ accessed 22 October 2024 13:30

carefully weigh the costs and benefits of such strategies, considering factors such as operational efficiency, compliance risk, and the specific requirements of their business models.[241]

8.4 Limitations of the Study

While this research provides valuable insights into GDPR compliance strategies and challenges for international corporations, it is important to acknowledge certain limitations:

Reliance on Publicly Available Information: The study primarily relied on publicly available information, including legal documents, corporate reports, and academic literature. While this allowed for a broad analysis, it may not capture the full range of internal practices and challenges faced by international corporations.

Rapidly Evolving Regulatory Landscape: The field of data protection law is rapidly evolving, with new interpretations, guidelines, and court decisions emerging regularly. Nevertheless, every attempt was made to include the information based on the most recent trends; however, some findings can be altered with the future changes in the regulation.

Focus on EU Law: Although the study looked at the impact of the GDPR globally, the research was mainly based on EU data protection law. The countries outside EU may not be presented to the full extent, their opportunities and issues might be completely different.

Limited Empirical Data: The study did not employ collection of primary empirical data using questionnaires or interviews with corporate data protection officers. It is regrettable that such data could have offered further information on the physical implementation of the GDPR.

Sector-Specific Nuances: Despite the fact that the study intended to give a general understanding of the GDPR compliance issues affecting the international corporations, the study may not be exhaustive in capturing the specific sectorial compliance issues.

8.5 Suggestions for Future Research

[241] W Kuan Hon, 'Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens' (Edward Elgar Publishing 2017). https://books.google.com/books?hl=en&lr=&id=hVXYDgAAQBAJ&oi=fnd&pg=PR1&dq=W+Kuan+Hon,+%27Data+Localization+Laws+and+Policy:+The+EU+Data+Protection+International+Transfers+Restriction+Through+a+Cloud+Computing+Lens%27+(Edward+Elgar+Publishing+2017).&ots=bML6dlsuZU&sig=oDBYIUv4XhVS6r8e_yPTZgayqrc accessed 22 October 2024 13:37

Based on the findings and limitations of this study, several avenues for future research can be identified:

Empirical Studies on Compliance Practices: Future research could benefit from empirical studies that directly engage with data protection professionals in international corporations. Surveys, interviews, or case studies could provide deeper insights into the practical challenges and effective strategies for GDPR compliance.

Comparative Analysis of Global Data Protection Regimes: A more comprehensive comparative analysis of data protection regimes worldwide, including emerging laws in countries like Brazil, India, and China, could provide valuable insights into the challenges of global data protection compliance.

Long-term Impact of *Schrems II*: As the implications of the *Schrems II* decision continue to unfold, longitudinal studies tracking its impact on international data flows and corporate compliance strategies would be valuable.

Effectiveness of Supplementary Measures: Research into the effectiveness of various supplementary measures implemented in response to *Schrems II* could provide practical guidance for organizations struggling with international data transfers.

Data Localization Trends: More research into the general trends toward data localization and the implications of this trend for both the functioning of global commerce and the effectiveness of data protection regimes might be valuable for policymakers and business executives.

Intersection of GDPR and Emerging Technologies: With emerging technologies such as artificial intelligence, blockchain technology, and the Internet of Things, research on the interaction of emerging technologies with GDPR can assist in future compliance issues.

Sector-Specific Compliance Strategies: It would be useful to investigate more detailed approaches to GDPR compliance by analysing success and failure factors in particular industries (e.g. healthcare, financial services, e-commerce).

In conclusion, this thesis has aimed to offer a detailed assessment of the approaches and issues that arise with the management of GDPR for cross-border data flows by international companies. The results prove the growing and multifaceted nature of the data protection issue

in the global environment, and therefore, require the implementation of systematic, dynamic and sensitive strategies and practises in managing the issue. In light of the developments in the digital economy and the continuous enhancement of data protection legislation, the research proposed in this paper will be imperative in order to safeguard personal data while at the same time promoting the advantages of cross-border data transfers.

Bibliography

Case laws

Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311

Statutes

California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (2018)

Cybersecurity Law of the People's Republic of China (2016) https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3

Federal Law No. 242-FZ, On Amendments to Certain Legislative Acts of the Russian Federation with Regard to Specifying the Procedure for the Processing of Personal Data in Information and Telecommunication Networks (2014)

Lei Geral de Proteção de Dados Pessoais (LGPD), Lei No. 13,709/2018 (2018)

Personal Information Protection Law of the People's Republic of China (2021)

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 L119/1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Books

Bradford A, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020) DOI: 10.1093/oso/9780190088583.001.0001

Bygrave LA, *Data Privacy Law: An International Perspective* (Oxford University Press 2014) http://dx.doi.org/10.1093/acprof:oso/9780199675555.001.0001

Custers B and others, *EU Personal Data Protection in Policy and Practice* (T.M.C. Asser Press 2019)

Hon WK, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens* (Edward Elgar Publishing 2017)

Kuner C, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013) https://doi.org/10.1093/acprof:oso/9780199674619.001.0001

Lynskey O, *The Foundations of EU Data Protection Law* (Oxford University Press 2015)

McLeod I, *Legal Method* (10th edn, Palgrave Macmillan 2019)

Moerel L, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (Oxford University Press 2012) https://doi.org/10.1093/acprof:oso/9780199662913.001.0001

Siems M and Yap PJ (eds), *The Cambridge Handbook of Comparative Law* (CUP 2024) https://books.google.com/books?id=TdPvEAAAQBAJ

Tamò-Larrieux A, *Designing for Privacy and its Legal Framework* (Springer 2018) DOI: 10.1007/978-3-319-98624-1

Voigt P and von dem Bussche A, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) http://dx.doi.org/10.1007/978-3-319-57959-7

Yin RK, *Case Study Research and Applications: Design and Methods* (6th edn, SAGE Publications 2017) https://www.google.com/books/edition/Case_Study_Research_and_Applications/6DwmDwAAQBAJ

Articles

Andraya Flor, 'The Impact of Schrems II: Next Steps for U.S. Data Privacy Law' (NDLScholarship) https://scholarship.law.nd.edu/ndlr/vol96/iss5/10/

Azzi A, 'The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 126

Bennett CJ, 'The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats' in Daniel Guagnin and others (eds), *Managing Privacy through Accountability* (Palgrave Macmillan 2012)

Bieker F and others, 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' (2016) 4 Privacy Technologies and Policy 21

Bradford L, Aboy M and Liddell K, 'Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II' (2021) 8 Journal of Law and the Biosciences https://doi.org/10.1093/jlb/lsab007

Braun V and Clarke V, 'Using thematic analysis in psychology' (2006) 3(2) Qualitative Research in Psychology 77

Brkan M, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core' (2018) 14 European Constitutional Law Review 332

Brkan M, 'The Court of Justice of the EU, Privacy and Data Protection: Judge-made Law as a Leitmotif in Fundamental Rights Protection' in Maja Brkan and Evangelia Psychogiopoulou (eds), *Courts, Privacy and Data Protection in the Digital Environment* (Edward Elgar Publishing 2017) https://doi.org/10.4337/9781784718718.00009

Cavoukian A and Castro D, 'Big Data and Innovation, Setting the Record Straight: De-identification Does Work' (2014) Information Technology and Innovation Foundation https://www2.itif.org/2014-big-data-deidentification.pdf

Chander A and Lê UP, 'Data Nationalism' (2014) 64 Emory Law Journal 677

Chander A, Kaminski ME and McGeveran W, 'Catalyzing Privacy Law' (2021) 105 Minnesota Law Review 1733 https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=4353&context=mlr

Chivot E and Castro D, 'What the Evidence Shows About the Impact of the GDPR After One Year' (Center for Data Innovation, 17 June 2019) https://datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/

Colonna L, 'Data Mining and EU Data Protection Law: Challenges for Big Data Analysis in the GDPR Era' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds), *New Technology, Big Data and the Law* (Springer 2017) DOI: 10.1007/978-981-10-5038-1_6

Felzmann H and others, 'Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns' (2019) 6 Big Data & Society

Finck M, 'Blockchains and Data Protection in the European Union' (2018) 4 European Data Protection Law Review 17

Gellert R, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection' (2016) 2 European Data Protection Law Review 481

Greze B, 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives' (2019) 9 International Data Privacy Law 109

Gürses S, Troncoso C and Diaz C, 'Engineering Privacy by Design Reloaded' (Amsterdam Privacy Conference, October 2015) https://software.imdea.org/~carmela.troncoso/papers/Gurses-APC15.pdf

Hon WK and Millard C, 'Banking in the Cloud: Part 3 -- Contractual Issues' (2018) 34 Computer Law & Security Review 595 https://doi.org/10.1016/j.clsr.2017.11.007

Hon WK and Millard C, 'Banking on the Cloud: Effects of Security, Privacy and Data Protection Laws on Cloud Use' (2018) 15 Journal of International Commercial Law and Technology 1

Hutchinson T and Duncan N, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17(1) Deakin Law Review 83

Irion K, 'Panta Rhei: A European Perspective on Ensuring a High-Level of Protection of Digital Human Rights in a World in Which Everything Flows' (30 June 2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3638864

Kuner C, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18 German Law Journal 881

Kuner C, 'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (OUP 2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890930

Kuner C, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (2020) 23 European Law Review 1

Kuner C, 'The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation' (2020) European Law Blog http://www.kuner.com/my-blog-entries.html

Mantelero A, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754

Moerel E, 'Binding Corporate Rules: Fixing the Regulatory Patchwork of Data Protection' (2011) 28 Chicago Journal of International Law 1

Moerel L, 'GDPR conundrums: The data transfer conundrum' (2020) 169 Computer Law & Security Review 1 https://assets.contentstack.io/v3/assets/blt5775cc69c999c255/blt4acf7754cc1e1db6/160719gdprconundrumsdpo.pdf

Online journals

Quelle C, 'The 'Risk Revolution' in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too' in Ronald Leenes and others (eds), *Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2018)

Rob van Eijk and Gabriela Zanfir-Fortuna, 'Schrems II: Article 49 GDPR Derogations May Not Be So Narrow and Restrictive After All?' (Future of Privacy Forum, 4 February

2021) https://fpf.org/blog/schrems-ii-article-49-gdpr-derogations-may-not-be-so-narrow-and-restrictive-after-all/

Svantesson DJB, 'European Union Claims of Jurisdiction over the Internet -- an Analysis of Three Recent Key Developments' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 113

Svantesson DJB, 'The Extraterritoriality of EU Data Privacy Law -- Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stanford Journal of International Law 53

Teixeira GA, da Silva MM and Pereira R, 'The Critical Success Factors of GDPR Implementation: A Systematic Literature Review' (2019) 21(4) *Digital Policy, Regulation and Governance* 402 https://doi.org/10.1108/DPRG-01-2019-0007

Tikkinen-Piri C, Rohunen A and Markkula J, 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 Computer Law & Security Review 134

Tosoni L, 'The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation' (14 May 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3845913

Van Alsenoy B, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 271

Van Hoecke M, 'Legal Doctrine: Which Method(s) for What Kind of Discipline?' in Mark Van Hoecke (ed), *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Hart Publishing 2011)

Voss WG, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29(3) Washington International Law Journal 485 https://digitalcommons.law.uw.edu/wilj/vol29/iss3/7/

Wachter S, Mittelstadt B and Floridi L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76

Yakovleva S and Van Hoboken J, 'The Algorithmic Learning Deficit: Artificial Intelligence, Data Protection, and Trade' [2020] SSRN Electronic Journal https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3668434

Zalnieriute M, 'Data Transfers After Schrems II: The EU-US Disagreements Over Data Privacy and National Security' (2022) 55 *Vand J Transnat'l L* 1 https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/vantl55&section=4

Zheng Z and others, 'An Overview on Smart Contracts: Challenges, Advances and Platforms' (2020) 105 Future Generation Computer Systems 475

Government reports

Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ('DPOs')' (WP 243 rev.01, 5 April 2017) https://ec.europa.eu/newsroom/just/document.cfm?doc_id=44100

Article 29 Data Protection Working Party, 'Working Document Setting Up a Table with the Elements and Principles to be Found in Binding Corporate Rules' (WP 256 rev.01, 6 February 2018) https://ec.europa.eu/newsroom/article29/redirection/document/49725

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 L199/31 https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

European Commission, 'Adequacy decisions' (European Commission) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

European Commission, 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework' (European Commission, 25 March 2022)

European Data Protection Board, 'Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems' (23 July 2020) https://www.edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en

European Data Protection Board, 'Guidelines 01/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679' (4 June 2019) https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en

European Data Protection Board, 'Guidelines 01/2022 on data subject rights - Right of access' (18 January 2022) https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

European Data Protection Board, 'Guidelines 02/2022 on the application of Article 60 GDPR' (14 March 2022) https://www.edpb.europa.eu/system/files/2022-03/guidelines_202202_on_the_application_of_article_60_gdpr_en.pdf

European Data Protection Board, 'Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation' (4 June 2019) https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (10 November 2020) https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en

European Data Protection Board, 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures' (10 November 2020)

European Data Protection Supervisor, 'Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies' (EDPS, 16 July 2019)

European Union Agency for Cybersecurity, 'Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity' (ENISA, December 2023) https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

European Union Agency for Cybersecurity, 'Data Pseudonymisation: Advanced Techniques and Use Cases' (ENISA, January 2024)

Information Commissioner's Office, 'Data Security Incident Trends' (ICO, Q3 2023-24) https://ico.org.uk/action-weve-taken/data-security-incident-trends/

Information Commissioner's Office, 'Documentation' (ICO) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

Information Commissioner's Office, 'Guide to Binding Corporate Rules' (ICO, 19 December 2023) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/guide-to-binding-corporate-rules/

Information Commissioner's Office, 'International Data Transfer Agreement and Guidance' (ICO, 2024) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

Others

Amazon Web Services, 'AWS Compliance' (AWS) https://aws.amazon.com/compliance/

Bird & Bird, 'Guide to the General Data Protection Regulation' (Bird & Bird, April 2023) https://iapp.org/resources/article/bird-bird-guide-to-the-general-data-protection-regulation/

'CIPL Issues White Paper on GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges' (Hunton Andrews Kurth Privacy & Information Security Law Blog, 6 June 2019) https://www.huntonak.com/privacy-and-information-security-law/cipl-issues-white-paper-on-gdpr-one-year-in-practitioners-take-stock-of-the-benefits-and-challenges

Deutsche Telekom, 'Data Privacy' (Deutsche Telekom, 2024) https://report.telekom.com/interim-report-q2-2024/services/privacy-policy.html

DLA Piper, 'DLA Piper GDPR fines and data breach survey: January 2024' (DLA Piper, January 2024) https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024

DLA Piper, 'GDPR Data Breach Survey 2022' (DLA Piper, January 2022) https://www.dlapiper.com/en/insights/publications/2022/01/dla-piper-gdpr-fines-and-data-breach-survey-2022/

EU Cloud Code of Conduct, 'About the EU Cloud Code of Conduct' (SCOPE Europe, 2024) https://eucoc.cloud/en/about/about-eu-cloud-coc/

European Institute of Public Administration, 'Data Protection Officer (DPO) Certification Training' (EIPA, 2024) https://www.eipa.eu/courses/data-protection-certification/

Gartner, 'Top Strategic Technology Trends for 2024' (Gartner, October 2023) https://tetrate.io/resource/gartner-top-strategic-technology-trends-for-2024-platform-engineering/#:~:text=2024%3A%20Platform%20Engineering-,Gartner%C2%AE%20Top%20Strategic%20Technology%20Trends%20for%202024%3A%20Platform%20Engineering,streamline%20application%20delivery%20by%202026

'GDPR conundrums: Data transfer' (IAPP, 9 June 2016) https://iapp.org/news/a/gdpr-conundrums-data-transfer

GlaxoSmithKline, 'Annual Report 2023' (GSK plc, February 2024) https://www.gsk.com/media/11007/annual-report-2023.pdf

GlaxoSmithKline, 'Digital Health and Data Science' (GSK plc, 2024) https://www.gsk.com/en-gb/

GlaxoSmithKline, 'Privacy Centre' (GSK plc, 2024) https://privacy.gsk.com/en-us/privacy-notice/

Google, 'Data Processing Amendment to Google Analytics Terms of Service' (Google, 2024) https://support.google.com/analytics/answer/3379636

IBM, 'IBM Data Privacy Services' (IBM, 2024) https://www.ibm.com/data-privacy

Information Commissioner's Office, 'Codes of Conduct and Certification' (ICO, 2024) https://ico.org.uk/for-organisations/advice-and-services/codes-of-conduct/

International Association of Privacy Professionals, 'The Schrems II Decision: EU-US Data Transfers in Question' (IAPP, 16 July 2020) https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question

KPMG, 'Schrems II: Impact and Challenges' (KPMG, September 2020)

Microsoft, 'Encryption in the Microsoft Cloud' (Microsoft Trust Center, 2024) https://learn.microsoft.com/en-us/purview/office-365-encryption-in-the-microsoft-cloud-overview

Moerel EML, 'Binding Corporate Rules: Fixing the Regulatory Patchwork of Data Protection' (PhD thesis, Tilburg University 2011) https://research.tilburguniversity.edu/files/1346784/Moerel_binding_19-09-2011.pdf

Nestlé, 'Privacy Notice' (Nestlé, 2024) https://www.nestle.com/info/privacy/privacy-notice

Novartis, 'Binding Corporate Rules' (Novartis, 2024) https://www.novartis.com/privacy#:~:text=To%20complement%20the%20Novartis%20Policy,is%20governed%20by%20the%20EU

OneTrust, 'Schrems II Solutions' (OneTrust, 2024) https://www.onetrust.com/solutions/schrems-ii-compliance/

'PECB GDPR Certified Data Protection Officer' (PECB African Training Institute) https://afralt.org/pecb-gdpr-certified-data-protection-officer/

Rolls-Royce, 'Annual Report 2023' (Rolls-Royce plc, March 2024) https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/annual-report/2024/2023-annual-report.pdf

Rolls-Royce, 'Data Privacy' (Rolls-Royce plc, 2024) https://www.rolls-royce.com/site-services/data-privacy.aspx

Rolls-Royce, 'Digital Innovation' (Rolls-Royce plc, 2024) https://www.rolls-royce.com/innovation/digital.aspx

Royal Dutch Shell, 'Privacy Policy' (Shell, 2024) https://www.mesc.shell.com/Content/HTML%20pages/PrivacyPolicy.html

Salesforce, 'Data Processing Addendum' (Salesforce, 2024) https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf

SAP, 'Data Processing Agreement for SAP Cloud Services' (SAP Trust Center, 2024) https://www.sap.com/africa/about/trust-center/agreements/on-premise/data-processing-agreements.html

SAP, 'SAP's Data Protection Impact Assessment Tool' (SAP Trust Center, 2024) https://www.sap.com/about/trust-center/data-protection-and-privacy.html

Telefónica, 'Global Privacy Policy' (Telefónica, 2021) https://www.telefonica.com/en/wp-content/uploads/sites/5/2021/03/global-privacy-policy.pdf

Tene O and Wolf C, 'Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation' (The Future of Privacy Forum, January 2013) https://fpf.org/wp-content/uploads/2013/01/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20131.pdf

'The Definitive Guide to Schrems II' (OneTrust DataGuidance, 22 November 2022) https://www.dataguidance.com/resource/definitive-guide-schrems-ii

'The impact of the 'Schrems II' case on personal data' (KPMG Law, 2020) https://kpmglaw.be/news/posts/2020/august/the-impact-of-the-schrems-ii-case-on-personal-data/

'The impact of the 'Schrems II' case on personal data' (KPMG Law, August 2020) https://kpmglaw.be/news/posts/2020/august/the-impact-of-the-schrems-ii-case-on-personal-data/

'What is confidential computing?' (IBM, 4 June 2024)
https://www.ibm.com/topics/confidential-computing