Cross-Border Transfers of Personal Data after Schrems II
Supplementary Measures and New Standard Contractual Clauses (SCCs)
Corrales Compagnucci, Marcelo; Aboy, Mateo; Minssen, Timo

Published in:
Nordic Journal of European Law

Publication date:
2022

Document version
Early version, also known as pre-print

Document license:
CC BY

Citation for published version (APA):
Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)

Marcelo Corrales Compagnucci, Mateo Aboy, Timo Minssen*

Abstract: This article analyses the legal challenges of international data transfers resulting from the recent Court of Justice of the European Union (CJEU) decision in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Schrems II). This judgement invalidated the EU-US Privacy Shield Framework but upheld the use of standard contractual clauses (SCCs). However, one caveat is that organisations would have to perform a case-by-case assessment on the application of the SCCs and implement ‘supplementary measures’ to compensate for the lack of data protection in the third country, where necessary. Regrettably, the CJEU missed the opportunity to specify what exactly these ‘supplementary measures’ could be. To fill this gap, the European Data Protection Board (EDPB) adopted guidelines on the measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. In addition, on June 4th, 2021 the European Commission issued new SCCs which replaced the previous SCCs that were adopted under the previous Data Protection Directive 95/46. These new developments have raised the bar for data protection in international data transfers. In this article, we analyse the current regulatory framework for cross-border transfers of EU personal data and examine the practical considerations of the emerging post-Schrems II legal landscape.

Keywords: Schrems II, international data transfers, supplementary measures, new Standard Contractual Clauses (SCCs), EDPB Recommendations 01/2020, encryption, security and organisational measures, GDPR.

1 Introduction

One explicit goal of the General Data Protection Regulation (GDPR)¹ is to guarantee the free flow of personal data between EU Member States. Additionally, the GDPR contemplates the possibility of transferring personal data to a third country – a country outside of the European Economic Area

* Marcelo Corrales Compagnucci is an Associate Professor at the Centre for Advanced Studies of Biomedical Innovation Law (CeBIL), Faculty of Law (UCPH); Mateo Aboy is a Principal Research Scholar in Biomedical Innovation, Precision Medicine, AI & Law at the Centre for Law, Medicine and Life Sciences (LML), Faculty of Law, University of Cambridge & Affiliated Professor & Fellow at CeBIL, Faculty of Law, University of Copenhagen (UCPH); Timo Minssen is a Law Professor and the Founding Director for the Centre for Advanced Studies of Biomedical Innovation Law (CeBIL), Faculty of Law (UCPH). He is also affiliated as a guest researcher with Lund University. This is a working paper version. The final version was submitted to the Nordic Journal of European Law.

(EEA) – or an international organisation, provided that importers and exporters can guarantee that data will be protected under the same European standards. GDPR provisions for international data transfers also include onward transfers. For instance, from a processor to a sub-processor in a third country outside the EEA.²

The current legal landscape to transfer personal data outside of the EEA as set out in the GDPR includes the following mechanisms:

i) **Adequacy decisions (Art. 45 GDPR).**

Adequacy decisions are based on assessments that third country laws and practices guarantee the same level of European standard protection. The effect of such decisions is that personal data can flow without restrictions and any further additional safeguards. In other words, transfers to the countries in this list will be assimilated to intra-EU transmissions of data.³

ii) **Appropriate safeguards (Art. 46 GDPR).**

In the absence of adequacy decisions, organisations involved in the cross-border transfers must implement ‘appropriate safeguards’ (ie, Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), codes of conducts, certification mechanisms and ad hoc contractual clauses) to ensure that the level of protection is not undermined.⁴

iii) **Derogations (Art. 49 GDPR).**

In the absence of an adequacy decision or appropriate safeguards, there are specific situations (eg, the transfer is necessary for important reasons of public interest) where derogations may be used but these have an exceptional nature and are subject to strict conditions such as occasional and non-repetitive processing activities.⁵

Recent developments, including the *Schrems II* decision, the follow-on European Data Protection Board (EDPB) Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data,⁶ and the new SCCs for the transfer of personal

---

⁴ See Art. 46 of the GDPR. The transfer tools may require additional ‘supplementary measures’ to ensure essentially equivalent level of protection. See C-311/18 (Schrems II), paragraphs 130 and 133.
⁵ See Art. 49 of the GDPR.
⁶ EDPB Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Adopted on 10 November 2020 [hereinafter EDPB Recommendations 01/2020], available
data to third countries issued by the European Commission (EC) on June 4th, 2021, have raised a wave of debates and concerns among data protection professionals.

While the Schrems II ruling ultimately found that the SCCs were valid, the Court also noted that the receiving country’s laws could potentially undermine the protections in the SCCs, exacerbating the uncertainties and risks for organisations relying on this transfer tool. The new SSCs provide more flexibility and ameliorate some of the shortcomings of the previous SCCs. They raise the standard of data protection and include stricter rules for data importers and exporters, in particular extensive obligations for data importers acting as controllers.

In light of these new challenges, this article aims to analyse the emerging legal framework for international transfers of personal data. The paper is structured as follows. Section 2 elucidates the background and main issues raised in the Schrems cases. Section 3 then provides a synopsis of the current legal framework and data protection guidance for cross-border transfers after the Schrems II judgment. This provides the basis for Section 4, which delivers a discussion of the practical implications of these developments including a discussion of how to best navigate the new legal environment for international data transfer. This will allow us to draw conclusions in Section 5.

2 The Invalidation of the Safe Harbour Agreement and the EU-US Privacy Shield in Schrems I & II

In 2013, Austrian citizen and privacy activist Maximilian Schrems filed a legal suit with the Irish Data Protection Commission (DPC) against Facebook (Schrems I) and requested to prohibit or suspend the transfer of his personal data from Facebook Ireland to the United States. He considered that the law and practice of the United States did not warrant adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities such as the US National Security Agency (NSA).

---


10 CJEU, C-362/14 of 6 October 2015, ECLI:EU:C:2015:650 – Maximillian Schrems vs Data Protection Commissioner (Schrems I).

The DPC, however, rejected the complaint on the grounds of, in particular, Decision 2000/520 (Safe Harbour Agreement) which ensured an adequate level of protection of personal data transferred between the EU and the US. Mr. Schrems contested the decision of the DPC and the Irish High Court referred the case to the CJEU for a preliminary ruling on the interpretation and validity of the Safe Harbour Framework.  

In addition to the lack of informed consent and the failure to provide legal remedies for individuals, Mr. Schrems argued that US surveillance laws (such as section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333) and US programs disclosed by the Snowden revelations such as PRISM, allowed US authorities to access personal data from US Big Tech companies. The CJEU agreed with the plaintiff and decided to overturn the Safe Harbour Agreement in 2015, thereby making illegal to transfer personal data under this framework. The CJEU held that this was a violation to European privacy laws and the fundamental principles enshrined in Articles 7, 8 and 47 of the Charter of Fundamentals Rights of the European Union (CFR).

After the invalidation of the Safe Harbour Agreement, Facebook and other companies then changed to the SCCs to claim legal basis for the transfer of personal data outside of the EU. The US and European authorities signed another agreement which would compensate the failings of Safe Harbour. This new agreement was the so-called EU-US Privacy Shield Framework, whereby US-based companies could join by committing to the framework requirements and by submitting a self-certification to the US Department of Commerce. The EU-US Privacy Shield Framework included a list of requirements such as the submission of a privacy policy with specific details. In general, the framework required greater transparency, oversight and redress mechanisms, including the creation of an ombudsman to investigate complaints as well as

---

arbitration and alternative dispute resolution (ADR) mechanisms. In effect, the Privacy Shield enabled EU to US cross-border transfers under Art. 45 GDPR (as a limited adequacy decision).

By an amended complaint in December 2015, Mr. Schrems challenged the validity of Facebook’s use of SCCs and requested the DPC to prohibit or suspend the transfer of his personal data to Facebook Inc. Finally, in July 2020, the CJEU in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Schrems II) rendered the EU – US Privacy Shield invalid and upheld the validity of the SCCs.

Nevertheless, the Court required a ‘case-by-case’ analysis on the application of the SCCs. Controllers and processors exporting data need to verify if the law and practice of the third country impinges on the effectiveness of the appropriate safeguards established in Art. 46 GDPR. It follows from the Schrems II judgement that data exporters need to implement ‘supplementary measures’ that fill the gaps and bring it up to the level required by EU law. Unfortunately, the CJEU did not define or specify what these ‘supplementary measures’ are. This permeated in heated debates and a wave of guidelines and recommendations on those additional safeguards.

3 Recent Developments After Schrems II

After the Schrems II decision, on November 10th, 2020, the EDPB issued a six-step-approach Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. The EDPB Recommendations are intended to help organisations comply with the requirements established by the CJEU in Schrems II. Following the Recommendations, on June 4th, 2021, the European Commission issued the long-awaited new SCCs for the transfer of personal data to third countries. These two new developments are further explained below:

3.1 EDPB Recommendations: A Six-Step Approach

---


The EDPB recommends organisations to follow six steps to transfer personal data to third countries outside of the EEA:

- **Step 1 – Know your data transfers:** Data exporters should be fully aware of their transfers of personal data to third countries, including onward transfers. Mapping and recording all data transfers can be a complex task, however, this is necessary to ensure an essentially equivalent level of protection wherever it is processed. Data exporters should record all processing activities, keep data subjects informed and make sure it is in line with the principle of data minimisation.

- **Step 2 – Identify the transfers tools you are relying on:** A second step is to identify the transfer tools set out in Chapter V of the GDPR including: a) adequacy decisions; b) transfers tools containing ‘appropriate safeguards’ of a contractual nature in the absence of adequacy decisions (such as SCCs, Binding Corporate Rules (BCRs), codes of conducts, certification mechanisms and ad hoc contractual clauses); and, c) derogations. If your data transfer does not fall under either a) ‘adequacy decisions’ or c) ‘derogations’, you need to continue to step 3.

- **Step 3 – Assess whether Art. 46 of the GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer:** Utilising a transfer tool under Art. 46 of the GDPR may not be sufficient if your transfer tool is not ‘effective’ in practice. ‘Effective’ means that the level of protection is essentially equivalent to that afforded in the EEA. Data exporters should carry out a Transfer Impact Assessment (TIA) to assess – in collaboration with the importer – if the law and practice of the third country where the data is being transferred may impinge on the effectiveness of the appropriate safeguards of the Art. 46 in the context of the specific transfer. In performing this assessment, different aspects of the third country legal system should be taken into account, in particular whether public authorities can access

---

23 EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (hereinafter ‘EDPB Recommendations 01/2020’) (adopted on 10 November 2020), 8-9.

24 See Art. 45 of the GDPR. Adequacy decisions may cover a country as a whole or be limited to a part of it. If you transfer data to any of these countries there is no need to take any further steps described in this section. The EU Commission has so far recognised only twelve countries which can offer adequate level of protection. These countries are: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. As of March 2021, adequacy talks were concluded with South Korea. See European Commission, Adequacy decisions, How the EU determines if a non-EU country has an adequate level of data protection, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed 9 October 2021.

25 Art. 46 of the GDPR. The transfer tools may require additional ‘supplementary measures’ to ensure essentially equivalent level of protection. See C-311/18 (Schrems II), paragraphs 130 and 133.

26 Art. 49 of the GDPR.

27 EDPB Recommendations 01/2020, 9-11.

28 See C-311/18 (Schrems II), paragraphs 105 and second finding.
personal data and, in general, those elements enlisted in Art. 45(2) of the GDPR\(^{29}\) such as the rule of law situation and respect for human rights in that third country.\(^{30}\)

- **Step 4 – Adopt supplementary measures:** If the TIA revealed that your Art. 46 tool is not ‘effective’, data exporters – in collaboration with the importers, where appropriate – need to consider if ‘supplementary measures’ exist. By definition, supplementary measures are ‘supplementary’ to the safeguards that the transfer tools already provides. In other words, if added to the safeguards contained in Art. 46, could ensure that the data transferred is afforded an adequate level of protection in the third country which is essentially equivalent to the European standard. Exporters need to identify on a case-by-case basis which supplementary measures could be effective taking into account the previous analysis in steps 1, 2 and 3.\(^{31}\)

- **Step 5 – Formal procedural steps:** Make sure to take any formal procedural steps in case you have identified effective supplementary measures, which may vary depending on the transfer tool used or expected to be used. For instance, if data exporters intend to put in place supplementary measures in addition to the SCCs, there is no need to request an approval from the supervisory authority as long as the supplementary measures do not contradict, directly or indirectly, the SCCs and are enough to ensure that the level of protection guaranteed by the GDPR is not compromised in any way.\(^{32}\)

- **Step 6 – Re-evaluate at appropriate intervals:** The last step put forward by the EDPB is to monitor and review, on an ongoing basis, if there are new developments in the third country where data was transferred which could affect the initial assessment of the level of protection of the third country and the supplementary measures taken based on the TIA and the specific transfer. This is also in line with the principle of accountability which is a continuous obligation as set out in Art. 5(2) GDPR. Data exporters, in collaboration with the importers, should put in place sufficiently sound mechanisms to ensure that any transfer relying on the SCCs are suspended or prohibited if the supplementary measures are no longer effective in that third country or where those clauses are breached or impossible to honour.\(^{33}\)

### 3.2 New Standard Contractual Clauses (SCCs)

SCCs have a dual nature as a private contract and public instrument granting enforceable GDPR rights to third parties and subject to the oversight of the EU data protection authorities. They are intended to provide ‘appropriate safeguards’ under Art. 46 GDPR by creating legal obligations on

---

\(^{29}\) C-311/18 (Schrems II), paragraph 104.  
\(^{30}\) EDPB Recommendations 01/2020, 12.  
\(^{31}\) EDPB Recommendations 01/2020, 15-17.  
\(^{32}\) EDPB Recommendations 01/2020, 17-18.  
\(^{33}\) EDPB Recommendations 01/2020, 18-19.
the exporters and importers to ensure an appropriate level of data protection and GDPR compliance with respect to personal data transferred to countries which do not have adequacy decision (Art. 45 GDPR). On June 4th, 2021, the European Commission released updated versions of the SCCs which reflect the GDPR requirements and take into account the legal analysis in the Schrems II decision. The Commission adopted two sets of SCCs, one for use between controllers and processors in the EU/EEA and one for the transfer of personal data to third countries.

The main innovations and salient points of the new SCCs can be summarised as follows:

- **A modular approach**: Contrary to the prior set of SCCs which offered restricted possibilities of data transfers and separate sets of clauses, the new SCCs provide more flexibility for complex processing chains through a ‘modular approach’. This means that data exporters and data importers can now choose the module that best applies to their needs within the same agreement. In addition to the previously existing options for data transfers scenarios from ‘controller to controller’ and ‘controller to processor’, there are now two more modules governing data transfers from ‘processor to processor’ and ‘processor to controller’.

- **Geographic scope of application**: The new SCCs have a broader scope of application in comparison to the older version which only allowed the data exporter be a party if it was established in the EEA. This created barriers for data export compliance where a data exporter was established outside of the EEA but still subject to the GDPR by virtue of the GDPR’s extraterritorial scope in Art. 3(2). According to the new SCCs, the data exporter can also be a non-EEA entity. This provision, along with the modular approach, allows to cater any kind of data transfer between parties, despite of their data processing role or place of establishment.

- **Multiparty clauses and docking clause**: The new SCCs allow for multiple data exporting parties to contract (eg, within corporate groups or party collaborations) and for new parties to be added

---

37 Module 1: controllers to controllers, Module 2: controllers to processors, Module 3: processors to processors and Module 4: processors to controllers.
38 This is, for example, when there is a processor such as a cloud service provider located in the EEA and transfers data to another processor such as an infrastructure provider in the US.
39 In this case, the data is transferred back to the controller (back to ‘its origin’). This is also sometimes referred as ‘reverse transfer’.
to them over time through the so-called ‘docking clause’ (Clause 7). This clause is optional and allows additional third parties which are not (yet) a part of the agreement to join and sign up with the agreement of the other parties without having to conclude separate contracts. Third parties may now join by completing the Appendix – with details of the transfer, technical and organisational measures implemented and a list of sub-processors where relevant – and sign Annex 1.A. This new mechanism provides a more flexible approach for the existing data processing practices, in particular in the context of acquisitions, additional corporate entities, and sub-processors.

- **Data Protection Impact Assessment (DPIA):** In response to the Schrems II ruling, companies must perform and document a mandatory DPIA that should include a data transfer impact assessment (TIA) and make it available to the competent supervisory authority upon request. The TIA should assess, for instance: i) whether the laws of the third country into which the data is imported could conflict with the SCCs and the GDPR, ii) whether any additional safeguards are necessary to enhance data protections (eg, implement supplementary technical measures). For example, a TIA should determine whether the data importer is subject to the US Foreign Intelligence Surveillance Act Section 702 (FISA 702). The TIA should be monitored on a continuous basis and updated in light of any changes in the laws of the third country.

- **Security measures:** Annex II of the new SSCs provides a more detailed list of examples of the technical and organisational measures necessary to ensure an appropriate level of protection, including measures to ensure the security of the data. While the list is non-exhaustive, it includes measures to provide assistance to the parties. According to Annex II, the technical and organisational measures must be described in ‘specific (and not generic) terms’. This includes, in particular, any relevant ‘certifications’ to ensure an appropriate level of security, taking into consideration ‘the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.’ The measures of pseudonymisation and encryption are at the top of the list.

---


45 See Annex II Standard Contractual Clauses.
There are several other new practical features in the new SCCs toolbox which provide more flexibility and legal certainty to the parties involved, such as the possibility to choose the governing law and jurisdiction of any EU Member State. This is particularly useful when the SCCs cover multiple international data transfers and servers are located in different countries. The new SCCs contain significantly more requirements and obligations for data exporters and importers, particularly for importers acting as controllers. This is also more in line with the GDPR requirements. The new SCCs include, for instance, obligations to give notice to data subjects and to notify personal data breaches to EU authorities.\(^\text{46}\)

### 4 Practical Considerations

The CJEU ruled in *Schrems II* that the SCCs remain as a valid cross-border transfer mechanism provided the parties involved in the transfer implement the necessary ‘supplementary measures’ whenever they are needed to ensure substantially equivalent data protection by providing ‘appropriate safeguards’ to rectify any data protection gaps that undermine equivalency in the third countries.\(^\text{47}\) Regrettably, the Court failed to provide any meaningful guidance about what specific supplementary measures might be required in this regard. In an attempt to fill this gap, the EDPB Recommendations provide a non-exhaustive list of factors to identify – in collaboration with the importer – which supplementary measures would be most effective in protecting the data transferred. The new SCCs provide a useful instrument to support cross-border data transfers in many situations (eg, cross-border transfers of clinical trial data).

SCCs are currently the primary mechanism for cross-border transfers of personal data among commercial entities. Unlike the country-specific adequacy rulings under Art. 45 GDPR which are at the purview of the Commission, SCCs were not designed as a stand-alone mechanism for data transfer based on the adequacy of data protection law in the country receiving the data. SCCs, and other Article 46 ‘appropriate safeguards,’ such as Binding Corporate Rules (BCRs), were intended to offer an *alternative and additive*, multi-layered standard for data protection that utilises 1) the data protection law of the third party and addresses any gaps with respect to GDPR by adding 2) a customisable combination of legal, technological (eg, security measures), and organisational commitments to establish a safe and secure environment for cross-border data transfer beyond the EEA for situations where the third country does not have adequacy decision under Art. 45 GDPR.\(^\text{48}\)

---


\(^{47}\) *Schrems II* at 103, 134.

The new SCCs are aligned with the GDPR and provide examples of technical and organisational measures in Annex III. They fill a long-existing gap in data protection law (since the former SCCs were adopted pre-GDPR), provide additional flexibility with regards to the permitted cross-border data-flows and help improve legal certainty for some international data transfers to third countries. It is expected that these modernised SCCs will enable businesses to account for a greater variety of complex data transfers and at the same time offering a safe exchange of personal data, adding uniformity and legal predictability to business transactions. That said, in situations where an importer is subject to FISA 702 or similar public surveillance questions still remain. Specifically, what supplementary measures would be considered sufficient in such situations by the supervisory authorities or CJEU? Arguably, in conjunction with the SCCs the controller should at least 1) implement robust data minimisation to ensure the absolute minimum data needed for processing is transferred to the third country, 2) completely de-identify and encrypt the data transferred to the third country (both in transit and at rest encryption), 3) keep the encryption and pseudonymisation keys in the EU/EEA under the legal, organisational, and technical control of an EU party not subject to FISA (or other surveillance regime), 4) consider implementing multi-party encryption and processing (eg, multi-party homomorphic encryption), 5) implement a full information security management system (ISMS) such as the ISO 27001, and 6) document all these measures as part of Annex III of the SCC.

The use of the term ‘supplementary measures’ by the CJEU is unfortunate, as all these measures are technically part of the SCC security annex and were already needed to comply with the Art. 32 GDPR security of processing in light of part of the risk-based assessment (eg, Art. 35 GDPR DPIA). Furthermore, pursuant to Art. 46 the SCC is the ‘appropriate safeguard’ and these so-called ‘supplementary measures’ are technically not ‘supplementary’. Instead, they are the same security measures that have always been documented and incorporated by reference as part of the SCCs.

In addition, organisations will have to pay particular attention to the new ISO 27701, which is the latest international standard for data privacy information management in the ISO 27000 series. It is a certifiable extension to the ISO 27001 that attempts to help organisations in meeting the GDPR requirements when implementing a comprehensive privacy information management system (PIMS). Organisations that have already implemented the ISO 27001 ISMS are advised to add privacy and data protection controls in ISO 27701 to ensure appropriate levels of data protection, especially when involved in cross-border transfers of personal data.

There is a limited number of technical measures that could help organisations using SCCs to provide the European level of protection when the data is flowing around the world and possibly

subject to public surveillance. These include 1) the use of robust end-to-end encryption with one or more independent EU/EEA-based trustees securely holding the keys, and 2) multi-party homomorphic encryption. Both of these security measures are technical controls and should be implemented within an overall ISMS and PIMS that is properly scoped and regulatory stress-tested (eg, subject to regular enhanced penetration testing). Additionally, it is important for the ISMS/PIMS to be independently audited (eg, subject to third-party ISO27001/27701 certification audits).

5 Conclusion

Arguably, the new SCCs raised the bar for data protection and security in international data transfers. Adopting and complying with this new legal framework may result in substantive legal, organisational and technical requirements for some parties. Businesses and organisations need to identify which transfer tools are already in place and be ready to migrate them to the new SCCs and working with data importers or exporters to ensure they are compliant. They should follow a risk-based approach and be ready to perform a DPIA and TIA taking into account the EDPB Recommendations and new SCCs requirements. Considering the increasing importance of data driven technologies and the global flow of data, as well as the ever-fiercer competition of emerging markets with less restrictive data protection regulations, it remains to be seen how these developments will affect the competitiveness of the European data innovation landscape and industry in a great variety of sectors.

Acknowledgments: The research of all three co-authors for this contribution was supported by a Novo Nordisk Foundation grant for a scientifically independent Collaborative Research Programme in Biomedical Innovation Law (Grant agreement number NNF17SA0027784). Timo Minssen’s Research has also been supported by the Wallenberg Foundations’ ‘Initiative for Humanistic and Social Scientific Research in AI and Autonomous Systems’ (WASP-HS), see: https://portal.research.lu.se/portal/sv/projects/the-quantum-law-project(4d675bed-6738-4f81-9b28-48746ada562b).html.

52 Information Security Management System (ISO 27001).
53 Privacy Information Management System (ISO 27701).