Cooley

What comes after Privacy Shield: Negotiating Cross Border Data Transfer with your Vendors

Our Panel

- **Courtney Barton**, Vice President & Senior Counsel, Privacy & Data Security, Global Compliance at Marriott International
- **Tyler Thompson**, ACC Colorado Chapter liaison and Colorado attorney
- **Cobun Zweifel-Keegan**, Deputy Director, Privacy Initiatives at BBB National Program
- **Moderator: Randy V. Sabett**, Special Counsel, Cooley LLP

Intro to Topic

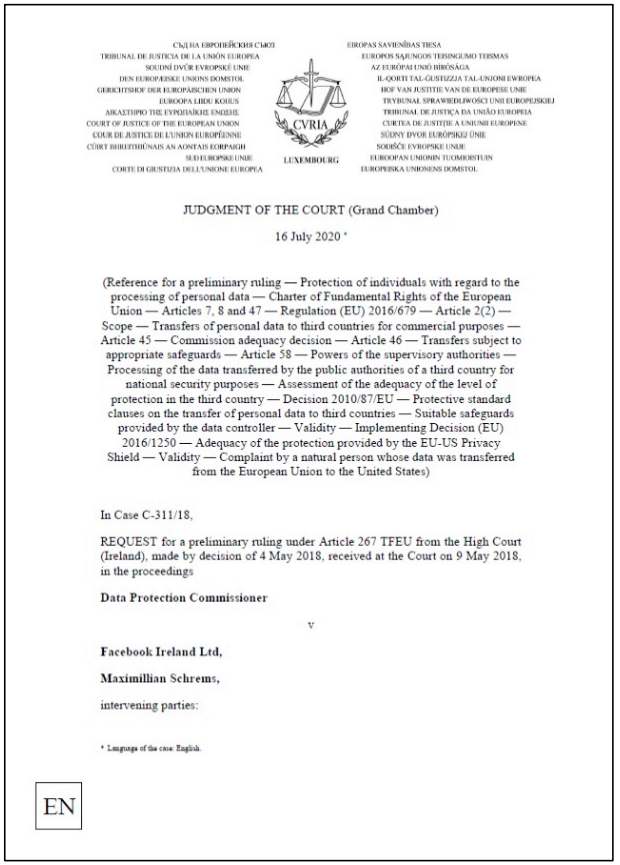
- What began over two years ago mainly as a “battle of the forms” to update terms of Data Protection Agreements for GDPR has now exploded into a complex discussion of how to address European personal data transfers in light of the Schrems II decision. With Privacy Shield now being invalidated and the EU Standard Contractual Clauses being called into question, companies now have an uncertain path forward for transferring personal data from Europe to the United States.

Schrems II

Cooley

What is *Schrems II*?

- A decision of the Court of Justice of the European Union ("CJEU") in the case, *Data Protection Commissioner v. Facebook Ireland, Ltd. and Maximillian Schrems* in which the CJEU:
  - invalidated the EU-US Privacy Shield framework; and
  - cast doubt on the viability of the so called Standard Contractual Clauses.
- Variety of drivers, including surveillance, FISA court, and EO 12333



СЪДЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL

CVRIA
LUXEMBOURG

JUDGMENT OF THE COURT (Grand Chamber)

16 July 2020 *

(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Regulation (EU) 2016/679 — Article 2(2) — Scope — Transfers of personal data to third countries for commercial purposes — Article 45 — Commission adequacy decision — Article 46 — Transfers subject to appropriate safeguards — Article 58 — Powers of the supervisory authorities — Processing of the data transferred by the public authorities of a third country for national security purposes — Assessment of the adequacy of the level of protection in the third country — Decision 2010/87/EU — Protective standard clauses on the transfer of personal data to third countries — Suitable safeguards provided by the data controller — Validity — Implementing Decision (EU) 2016/1250 — Adequacy of the protection provided by the EU-US Privacy Shield — Validity — Complaint by a natural person whose data was transferred from the European Union to the United States)

In Case C-311/18,

REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 4 May 2018, received at the Court on 9 May 2018, in the proceedings

Data Protection Commissioner

v

Facebook Ireland Ltd,

Maximillian Schrems,

intervening parties:

* Language of the case: English.

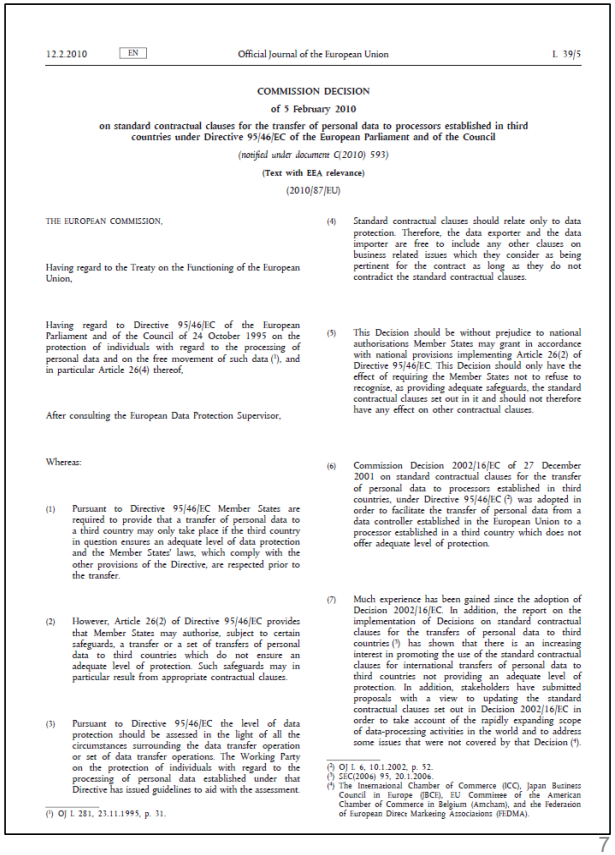
EN

What did the court decide in *Schrems II*?

- The CJEU invalidated the Privacy Shield framework, finding that the Privacy Shield did not offer an adequate level of protection for data transferred to the US. The CJEU's decision was based on the following findings:
  - US public authorities, including intelligence authorities, retain wide-ranging access to data transferred under Privacy Shield;
  - The Privacy Shield's Ombudsperson function does not provide adequate redress for EU residents affected by the transfer; and
  - The Privacy Shield's Ombudsperson is not empowered to adopt decisions that bind US intelligence services.

Did *Schrems II* invalidate Standard Contractual Clauses (SCCs) too?

- The CJEU concluded that the C2P SCCs remain a theoretically valid as a potential transfer mechanism.
- The CJEU did not state in specific terms that the C2P SCCs could not be validly used as a legal basis for transfers from the EU to U.S.-based importers.
- More later…



12.2.2010 EN Official Journal of the European Union L 39/5

COMMISSION DECISION

of 5 February 2010

on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

(notified under document C(2010) 593)

(Text with EEA relevance)

(2010/87/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1), and in particular Article 26(4) thereof,

After consulting the European Data Protection Supervisor,

Whereas:

(1) Pursuant to Directive 95/46/EC Member States are required to provide that a transfer of personal data to a third country may only take place if the third country in question ensures an adequate level of data protection and the Member States' laws, which comply with the other provisions of the Directive, are respected prior to the transfer.

(2) However, Article 26(2) of Directive 95/46/EC provides that Member States may authorise, subject to certain safeguards, a transfer or a set of transfers of personal data to third countries which do not ensure an adequate level of protection. Such safeguards may in particular result from appropriate contractual clauses.

(3) Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding the data transfer operation or set of data transfer operations. The Working Party on the protection of individuals with regard to the processing of personal data established under that Directive has issued guidelines to aid with the assessment.

(4) Standard contractual clauses should relate only to data protection. Therefore, the data exporter and the data importer are free to include any other clauses on business related issues which they consider as being pertinent for the contract as long as they do not contradict the standard contractual clauses.

(5) This Decision should be without prejudice to national authorisations Member States may grant in accordance with national provisions implementing Article 26(2) of Directive 95/46/EC. This Decision should only have the effect of requiring the Member States not to refuse to recognise, as providing adequate safeguards, the standard contractual clauses set out in it and should not therefore have any effect on other contractual clauses.

(6) Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (2) was adopted in order to facilitate the transfer of personal data from a data controller established in the European Union to a processor established in a third country which does not offer adequate level of protection.

(7) Much experience has been gained since the adoption of Decision 2002/16/EC. In addition, the report on the implementation of Decisions on standard contractual clauses for the transfers of personal data to third countries (3) has shown that there is an increasing interest in promoting the use of the standard contractual clauses for international transfers of personal data to third countries not providing an adequate level of protection. In addition, stakeholders have submitted proposals with a view to updating the standard contractual clauses set out in Decision 2002/16/EC in order to take account of the rapidly expanding scope of data-processing activities in the world and to address some issues that were not covered by that Decision (4).

(1) OJ L 281, 23.11.1995, p. 31.

(2) OJ L 6, 10.1.2002, p. 52.

(3) SEC(2006) 95, 20.1.2006.

(4) The International Chamber of Commerce (ICC), Japan Business Council in Europe (JBCE), EU Committee of the American Chamber of Commerce in Belgium (Amcham), and the Federation of European Direct Marketing Associations (FEDMA).

What about transfers from Switzerland and Great Britain to the US?

- *Schrems II* is binding only in the EU and did not apply to the Swiss-US Privacy Shield. However, on September 8, 2020, the FDPIC also opined that the Swiss-US Privacy Shield is inadequate for transfers from Switzerland to the US. While the FDPIC does not have authority to invalidate the Swiss-US Privacy Shield, in practice, its announcement casts serious doubt on the validity of that framework.
- Under the EU-UK Withdrawal Agreement, the UK is bound by the *Schrems II* decision until December 31, 2020. After that time, it is possible that the UK will follow the decision with respect to UK-US transfers. Any new U.K.-U.S. trade agreement is likely to address data transfers.

How were cross-border data transfers legitimized before the *Schrems II* decision?

- Before *Schrems II*, the two primary vehicles for lawful cross-border data transfers to the US were:
  - **Privacy Shield.** Ensuring that the recipient was certified to the US-EU Privacy Shield and the Swiss-US Privacy Shield, both administered by the United States Department of Commerce.
  - **Standard Contractual Clauses.** Execution by the importer and exporter of the personal data of the "Standard Contractual Clauses" for transfers of personal data adopted by the European Commission.
- There are other mechanisms that permit cross-border transfers under the GDPR, including binding corporate rules and derogations under GDPR. However, they are difficult to implement and/or rely on for various reasons and have not been broadly utilized to date.

Schrems II...and "adequacy"

Cooley

How are cross-border data transfers from Europe restricted?

- Article 45(1) of the EU General Data Protection Regulation ("GDPR") provides that transfers of data to a third country may only occur if that country has been deemed to "ensure[] an adequate level of protection" for personal data by the European Commission.
- Article 7 of the Swiss Federal Act on Data Protection ("FADP") restricts transfers of personal data from Switzerland to non-adequate countries. If the country to which the personal data will be transferred has not been deemed adequate, another mechanism must be used to make the transfer lawful under the GDPR and the FADP.

Which countries/territories have been deemed "adequate"?

- The European Commission has issued adequacy determinations for Andorra, Argentina, Canada (with respect to commercial organizations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.
- The FDPIC has issued adequacy determinations for Andorra, Argentina, Canada (with respect to commercial organizations), the EU (with respect to personal data of individuals only), the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand and Uruguay.

Have EU regulators indicated what "additional safeguards" might be required for SCCs to be "adequate"?

- To date, the Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemburg ("LfDI"), data regulator in the German state of Baden-Württemberg, has been the only EU regulator to issue guidance on using SCCs. According to the LfDI, companies should take the following extra precautions:
  - **Encrypt the data** in a manner in which "only the data exporter has the key" and the key cannot be broken by US intelligence authorities, or anonymize or pseudonymize the data in a way that only the data exporter can re-identify it;
  - Supplement the terms of the SCCs to require the **data importer to inform** the data exporter and the data subjects **of any legally binding requests for data by an enforcement authority**;
  - Supplement the terms of the SCCs to require the **data importer to contact the LfDI regarding such requests in the event that notification of the data exporter and the data subjects is prohibited** (for example, under criminal law); and
  - **Agree that any third-party beneficiary rights** invoked by data subjects be exercised in the courts of the EU Member State in which the data exporter is established.
- In practice, few US companies have a business model that would allow them to offer the encryption solution urged by the LfDI.

How can companies transfer data to US after *Schrems II*?

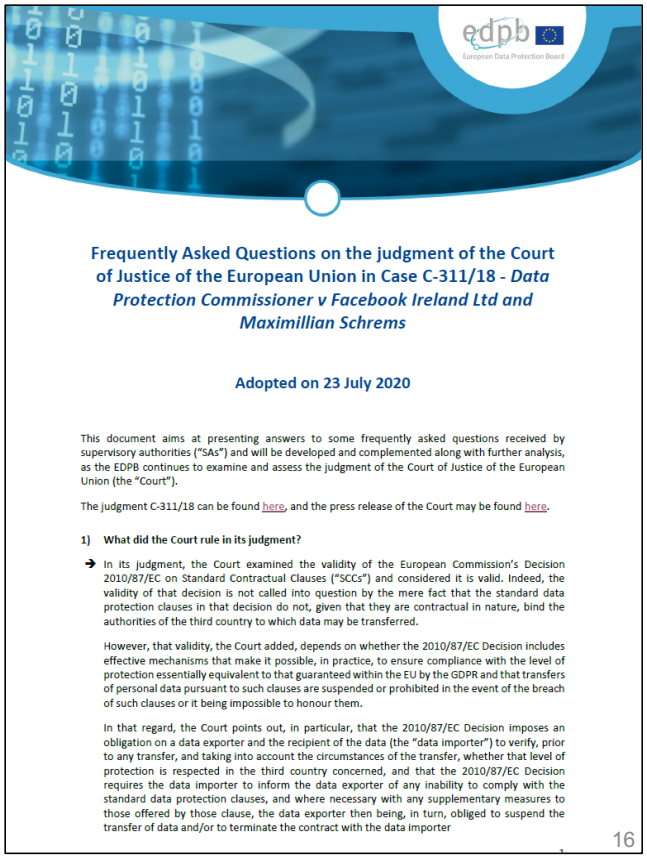
- Cross-border data flows from the EU to the US will continue. Currently, however, the Privacy Shield frameworks are invalid. Companies that previously relied on Privacy Shield for transfers to the US must transition to another mechanism to legitimize data transfers.
  - Relying on consent of the data subject is time consuming and probably impractical in most cases.
  - Binding corporate rules must be approved by the European Commission – an expensive and time-consuming process.
  - Derogations under GDPR Article 49 are difficult to rely on except for infrequent transfers.
- Until new frameworks are negotiated, or until the European Commission offers additional guidance on transfers to the US, **SCCs remain the most viable method for such transfers.**
- However, in entering into the SCCs, data exporters must be careful to comply with the *Schrems II* decision. In doing so, **data exporters must carefully consider what additional safeguards – including those suggested by the LfDI – may be sufficient in the context of that particular data transfer** in order to offer protection to the personal data at issue that is "essentially equivalent" to the protections provided by the GDPR.

Discussion Topic: Guidance

Cooley

EU Guidance

- The EDPB published FAQs immediately after the *Schrems II* decision. Focused on high-level reactions:
  - Privacy Shield is invalid for ongoing transfers
  - SCCs require additional safeguards
  - Art. 49 derogations are available
- Repeated that Sec. 702 FISA and EO 12333 do not allow for equivalent levels of protection
- Additional guidance from European DPAs has not been forthcoming, but it is likely coming soon.



edpb
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*

Adopted on 23 July 2020

This document aims at presenting answers to some frequently asked questions received by supervisory authorities ("SAs") and will be developed and complemented along with further analysis, as the EDPB continues to examine and assess the judgment of the Court of Justice of the European Union (the "Court").

The judgment C-311/18 can be found here, and the press release of the Court may be found here.

1) What did the Court rule in its judgment?

→ In its judgment, the Court examined the validity of the European Commission's Decision 2010/87/EC on Standard Contractual Clauses ("SCCs") and considered it is valid. Indeed, the validity of that decision is not called into question by the mere fact that the standard data protection clauses in that decision do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred.

However, that validity, the Court added, depends on whether the 2010/87/EC Decision includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection essentially equivalent to that guaranteed within the EU by the GDPR and that transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them.

In that regard, the Court points out, in particular, that the 2010/87/EC Decision imposes an obligation on a data exporter and the recipient of the data (the "data importer") to verify, prior to any transfer, and taking into account the circumstances of the transfer, whether that level of protection is respected in the third country concerned, and that the 2010/87/EC Decision requires the data importer to inform the data exporter of any inability to comply with the standard data protection clauses, and where necessary with any supplementary measures to those offered by those clause, the data exporter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the data importer

U.S. Guidance

- On Sept. 28, the U.S. Department of Commerce published a unique "whitepaper"
  - *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*
- On its face, the whitepaper focuses on helping U.S. businesses conduct the newly required case-by-case analysis for EU-U.S. transfers under SCCs and BCRs
- Does not interpret EU law, but does provide a different set of facts—updated beyond 2016—for companies to use in analyzing their surveillance risk, e.g.
  - Broader supervisory role for Foreign Intelligence Surveillance Court
  - Published targeting procedures
  - Additional layers of oversight
  - More redress for individuals than the CJEU acknowledged

Discussion Topic: What to do Moving Forward from *Schrems II*

Cooley

Establish alternative transfer mechanisms

- Both importers and exporters who rely on the Privacy Shield as the basis for transfers of personal data from the UK / EEA to certain U.S. organizations need to establish an alternative legal basis for those transfers under Chapter V of the GDPR.
- Depending on the circumstances, possible transfer mechanisms include:
  - execution of the appropriate form of Standard Contractual Clauses (however, see below for more on the C2P SCCs);
  - Binding Corporate Rules;
  - procuring data subject consent; or
  - reliance on another Article 49 derogation that might be available in respect of non-recurring transfers.

Enforcement grace period unlikely

- Following the CJEU's 2015 declaration that the US Safe Harbor decision was invalid in 2015, EU regulators granted an initial grace period of approximately four months, during which they agreed not to enforce that decision.
- This time, the FAQs from the EDPB indicated that there would be **no grace period** during which an organization can keep on transferring data to the United States without assessing its legal basis for the transfer.
- In practice, enforcement will depend on many factors – likely to be focused on EU exporters.
- DPAs differ widely in their prioritization of this enforcement area. The UK ICO issued an initial high-level statement on the decision (see here), in which it states that it "will be working with UK Government and international agencies to ensure that global data flows may continue".

Can the Privacy Shield be saved or could there be a Privacy Shield 2.0?

- In light of the fundamental nature of the apparent conflicts between the U.S. and EU laws concerned – it is unclear how the issues raised in the Decision could be solved without material (and in the current geo-political climate unlikely) concessions by either or both of the U.S. and/or the EU.
- That said, both sides have indicated that they are committed to finding a new solution.
- In the event that an agreement is reached, it is likely to look similar to the Privacy Shield Framework. The structure of Privacy Shield on the commercial side was not challenged.

Check contractual commitments

- Organizations should review their contracts with third parties to check the impact (if any) of Privacy Shield invalidity on contractual commitments made to third parties.
- To the extent needed and depending on the alignment of you company or client, consider a form amendment that would bring in additional safeguards that may not already be in the contract and add SCCs

What about Law Enforcement Considerations?

- Consider creating a law enforcement request policy to help serve as additional safeguards, aid in addressing the issue of law enforcement requests, and providing transparency regarding them. Such a policy could contain:
  - High level explanation of different possible requests
  - Requirement to consult legal, and how that will be done
  - Confirming request requirements (is it compulsory) and authenticity
  - Determining possible exceptions that may apply
  - Discussion on contesting requests, when applicable

Law Enforcement Considerations (cont'd)

- Additional points that a law enforcement request policy could contain:
  - Discussion on notify individuals to reduce privacy impacts
  - Possibly *require* that the Company notify an individual before their information is disclosed, unless prohibited by law
    - Note that while this may help with GDPR compliance, such a bright line may backfire in certain scenarios:
      - What if a government agency requests information of a large amount of individuals, will the company notify all of them?
  - Non-privacy concerns
- Perhaps consider a "Law Enforcement Impact Analysis"?

Discussion Topic: The Continuing Role of DPAs

Cooley

What about DPAs?

- Distinction between DPA and a Data Transfer Agreement
- Controllers almost always have data when dealing with vendors
- One option: include data protection terms in new standard agreements; DPAs came into play as a result of GDPR
- Ongoing uncertainties (e.g., SCC updates) will result in continued refinement of advice on this going forward

What is a DPA Playbook?

- Guide for use when negotiating a DPA
- Intended to accelerate contracting time by reducing the Privacy Function input needed to close a contract
- Identifies concessions that can be made without explicit Privacy Function approval
- A ‘living’ document that evolves to address commonly negotiated provisions

What the Vendor DPA Playbook **IS NOT**:

- NOT the final word on what privacy terms are acceptable.
- Concessions not permitted by playbook may be appropriate for business reasons. Contact the Privacy Function for guidance.
- NOT intended to discourage consultation with Privacy Function – they are always available to help.

Example: Security Breaches and Incident Response

Ref	Standard Language
3.4	Service Provider shall notify Customer immediately (but in no case later than 24 hours) after learning of a Security Incident. Notification must include a phone call to Service Provider's primary account contact. If Service Provider is unable to reach such contact promptly, Service Provider must contact Customer's Privacy Office at privacy@CUSTOMER.com. Notification shall include at a minimum (a) a description of the Incident including impact and likely consequences thereof, (b) the expected resolution time (if it has not already been resolved), (c) corrective measures to be taken, evaluation of alternatives, and next steps, and (d) the name and phone number of the Service Provider representative that Customer may contact to obtain further information and updates.
3.5	Without limitation of the foregoing, Service Provider shall promptly provide Customer with the following information as it becomes available: (a) a detailed description of the nature of the Security Incident, including where possible the categories and approximate number of Data Subjects and Personal Data records concerned; (b) a description of the measures taken or proposed to be taken to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects; and (c) whether any regulatory authority, the Data Subjects or the media have been informed or are otherwise already aware of the Security Incident, and their response.

Example: Security Breaches and Incident Response

Common Vendor Challenges/Requests	Rationale for Standard Language/Position
1. 24 hours is unreasonably fast. Increase to 72 hours or more. 2. Cannot commit to providing details of the incident. This may hamper the recovery of the Personal Data and/or the investigation into the incident or may not be permitted under applicable law.	1. We have legal obligations to notify authorities and/or affected individuals of Security Incidents on tight deadlines. EU: GDPR Art 33(2) requires Service Provider to notify us of Security Incidents. Art 33 also requires us to notify supervisory authorities of Personal Data Breaches within 72 hours. To meet this very tight deadline, we must receive Service Provider's notice no later than 24 hours after it learns of the incident so that we can investigate, coordinate with Service Provider and prepare the notice. 2. We need details of the incident to comply with our legal obligations to notify authorities and affected individuals about security incidents. EU: This information is required by GDPR Art 33(3) and Art 28(3)(f).

Discussion Topic: The Effect of *Schrems II* on M&A, Financing, IPOs, etc.

Cooley

Impact on risk factor disclosures

- U.S.-listed public companies would be well advised to update, or consider adding, specific risk factor disclosures in SEC filings, investor prospectuses and similar disclosures.
- Any such risk factors should identify the potential impact of Privacy Shield invalidation on the relevant organization's cross-border data transfers, as well as the nature, costs and difficulty of any associated rectifying measures that may be required.

Additional diligence required

- A determination must be made as to what mechanisms target used prior to *Schrems II* for cross border data transfer.
- Analyze current use of standard contractual clauses and any plans for expanding/augmenting/revamping.
- Review contracts with third party service providers and data handling companies.

Q&A

Cooley

Wrap Up

Cooley