Cooley

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Cybersecurity and Privacy Issue-Spotting in Vendor Agreements and Standard Contractual Clauses Post Schrems and CCPA

Presented by:
Toke Vandervoort
Sandeep Kathuria
Randy V. Sabett

December 9, 2021

Our Panel

Toke Vandervoort
Chief Legal Officer
Environmental Defense Fund

Sandeep Kathuria
Assistant General Counsel
Leidos

Randy V. Sabett
Special Counsel
Cooley

Our Landscape…in 90 minutes

- "The Way We Were"
  - Use of secure service providers (GLBA) or Business Associates (HIPAA) for handling sensitive information
  - More recently: Safe Harbor, Privacy Shield, and Standard Contractual Clauses
- Where are we today?
  - Security and privacy are top issues for most organizations
  - CCPA, GDPR, DPAs, and Standard Contractual Clauses
- Where are we going?
  - Worldwide changes, including new SCCs
  - Special use case: forensics and privilege concerns
- What about the government contracts industry approach?

The Way Were

Cooley

’90s & 00’s Security Mandates (Many Are Still in Play)

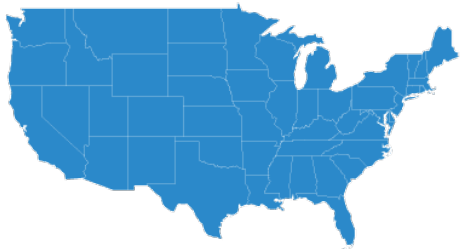
- These include:
  - HIPAA
  - GLBA
  - PCI
  - FAR/DFARS
  - Safe Harbor
  - Privacy Shield
  - Standard Contractual Clauses
  - Telecomm Rule

Where Are We Today

Cooley

Privacy & Security Requirements Changing Worldwide

- 50 state breach notification laws followed by:
  - CCPA and CPRA (California)
  - CPA and CDPA (Colorado and Virginia in 2023)
- Privacy Directive followed by:
  - GDPR (EU)
  - Schrems I and Schrems II (EU)
- FAR/DFARS followed by:
  - CMMC
- Others:
  - PIPL (China)
  - LPQD (Brazil)



Privacy & Security Requirements Changing Worldwide – Some DIB Observations (cont'd)

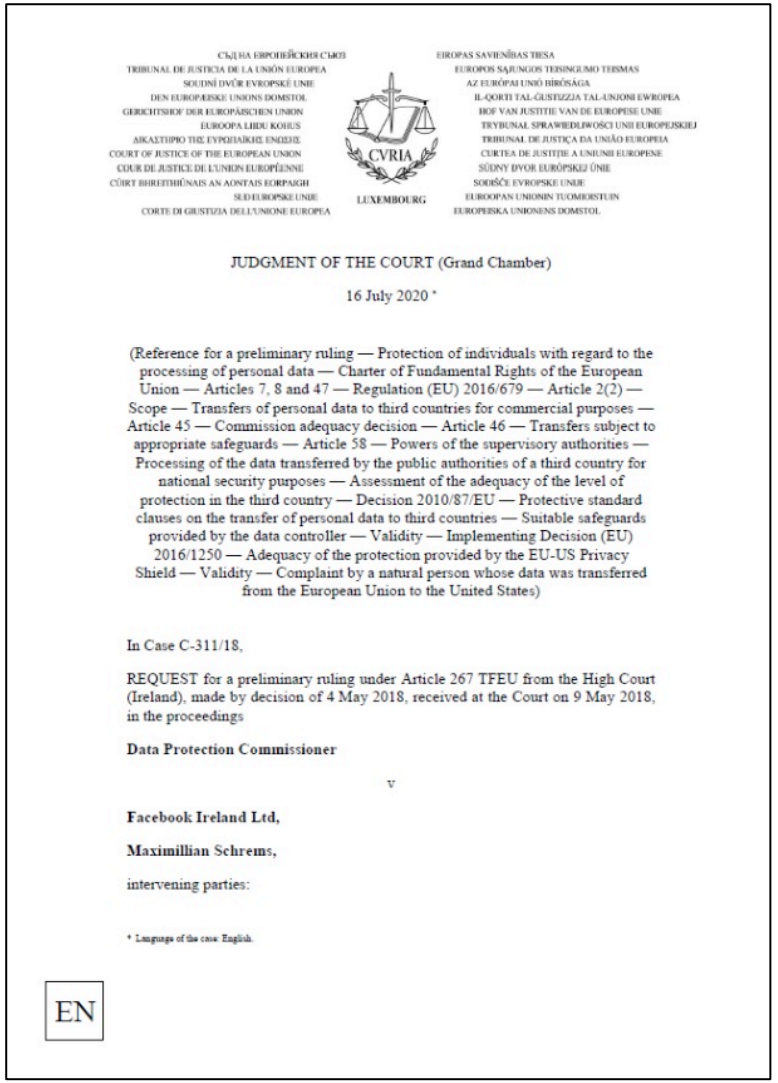
- Vendor due diligence in the commercial world shares some common aspects with, but also differs from, the supply chain risk management processes employed in the defense industrial base (DIB)
- Standard contract clauses for cybersecurity that are in the DoD supplement to the Federal Acquisition Regulation (i.e. the DFARS)
- In the DIB (and elsewhere) there are advantages and disadvantages of having and using a playbook.
- There are a wide variety of clauses and requirements that we see in the government contracts industry related to incident response there is a need for harmonization
- We'll be exploring these further as we proceed through the discussion

What To Consider in Moving Forward from *Schrems II*

Cooley

GDPR and *Schrems II*

- Schrems II was 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.



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

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

- No. However, the court did cast doubt on the SCCs' validity for purposes of transfers to the US.
- The CJEU opined that the validity of SCCs will depend on an evaluation by the data exporter regarding whether the SCCs ensure a level of protection "essentially equivalent" to the GPDR in the context of the particular transfer at issue.
  - The data exporter must consider the terms of the SCCs and the legal system of the recipient country, particularly with respect to access by public authorities to the transferred data and the remedies available to the affected individuals with respect to such access.
  - The data exporter must also consider whether "additional safeguards" should be included to supplement the provisions of the SCCs to ensure an adequate level of protection for the personal data being transferred.

New Standard Contractual Clauses

- New SCCs introduced by European Commission on June 4, 2021
  - Differences between the two new sets of SCCs:
    - Template contract for Art. 28
    - Covers transfers of personal data outside EEA
  - Main changes introduced include more data transfer scenarios, alignment with GDPR (transparency, DSRs, data breaches, etc.), data transfer impact assessment, and onward transfer clarity

When to start using the new SCCs

- The old SCCs have been repealed with effect from September 27, 2021:
  - Contracts concluded after that date must incorporate the new SCCs
- Contracts concluded before then, based on the old SCCs, will have a grace period of 15 months (until December 27, 2022), unless:
  - The parties change the agreement incorporating the old SCCs in a way that affects the processing conducted
- If no such changes are made, the agreements will still need to be updated with new SCCs by December 27, 2022

Next steps

- New SCCs provide that both parties must conduct a data protection impact assessment
- To prepare:
  - Start mapping your data flows to flag any new data transfers
  - Review existing agreements based on the old SCCs
  - Put a project plan in place involving key stakeholders and identifying tasks and timelines

Check contractual commitments and consider an explicit law enforcement policy

- Organizations should review contracts with third parties to check the impact (if any) of Privacy Shield invalidity and new SCCs
- Consider a law enforcement request policy to help serve as an additional safeguard, address law enforcement requests, and provide 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

CCPA

Cooley

What is a "sale" of personal information under CCPA?

*"**Sell**"...means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.*

- Exceptions for sharing with:
  - Certain affiliates (with same branding)
  - Service providers (if service necessary for business purpose and service provider contractually prohibited from using PI except to provide service)
  - Acquirers in M&A and similar transactions (but notice required if they make different use of PI)
- Implications
  - Most other commercial relationships caught in "sale" restrictions
  - Targeted online advertising = "sale"
  - Data brokerage = "sale"
  - Need to ensure vendor contracts contain required terms

What Must Businesses Do To Comply?

Notice & Transparency

Update privacy policy to provide required disclosures

Put Do Not Sell My Personal Information link on home page to enable opt-outs if PI sold

Provide privacy notice at or before point of PI collection, including in-app, at brick and mortar stores, and by phone

Establish mechanisms to accept requests to exercise individual rights

Give explicit notice and opportunity to opt out of PI resale

Individual Rights

Build mechanisms to receive CCPA requests

Honor Californians' rights to know, deletion, sales opt-out, non-discrimination

Verify requester's identity

Train relevant personnel to assist individuals with CCPA requests

Consent

Obtain prior opt-in consent to enter consumer into financial incentive (e.g., rewards) programs

Obtain "affirmative authorization" to sell PI of minors - from minor if under 16 and of parent if under 13

Avoid asking for opt-in consent to sell PI for 12 months after opt out

Vendor Management

Add data use restrictions to vendor contracts as necessary so they can qualify as CCPA "service providers"

Sample CCPA Contract Provisions

- Sale
  - *Notwithstanding anything to the contrary in this Agreement, the parties acknowledge and agree that the exchange of Personal Information between the parties in connection with this Agreement does not form part of the consideration exchanged between the parties in respect of this Agreement or any other business dealings*
- Personal Information
  - *"Personal Information" means any information about an identified or identifiable natural person and any other information that constitutes personal information as defined in the California Consumer Privacy Act of 2018 (as amended from time to time).*
- Service Provider
  - *Vendor shall not retain, use, or disclose Customer Personal Information for any purpose other than for the specific purpose of performing the Services specified in the Agreement [for the Customer, including retaining, using, or disclosing the Customer Personal Information for a commercial purpose (as defined in CCPA) other than providing the Services specified in the Agreement].*

Sample CCPA Contract Provisions

- Third Party
  - *Vendor shall not sell (as defined in CCPA) any Customer Personal Information or retain, use or disclose any Customer Personal Information for any purpose other than for the specific purpose of performing the Services specified in the Agreement[, including retaining, using, or disclosing the Customer Personal Information for a commercial purpose (as defined in the CCPA) other than provision of the Services], which for the avoidance of doubt also prohibits Vendor from retaining, using, or disclosing Customer Personal Information outside of its direct business relationship with Customer or for any other commercial purpose (as defined in the CCPA). Vendor certifies that it understands and will comply with the foregoing restrictions.*
- Anonymized Data
  - *Vendor may create and derive from Customer Personal Information data that (a) constitutes "aggregate consumer information" or has been "deidentified" (as such terms are defined in CCPA), and (b) does not constitute Confidential Information of Customer or identify Customer or any natural person ("Anonymous Data"), and use, publicize or share with third parties such Anonymous Data to improve Vendor's products and services and for its other legitimate business purposes. Vendor acknowledges that for purposes of this Agreement, Customer Personal Information has not been "deidentified" (as defined in CCPA) unless Vendor satisfies the same conditions for use of deidentified data applicable to a businesses under CCPA.*

Sample CCPA Contract Provisions

- Analytics and Other Uses
  - *The parties acknowledge and agree that the Services encompass Vendor's performance of its obligations and exercise of its rights under this Agreement.*
  - *Vendor will process Personal Data only in accordance with Client's instructions. By entering into this Addendum, Client instructs Vendor to process Personal Data to provide the Service. Client acknowledges and agrees that such instruction authorizes Vendor to process Personal Data (a) to perform its obligations and exercise its rights under the Agreement; (b) to perform its legal obligations and to establish, exercise or defend legal claims in respect of the Agreement; (c) pursuant to any other written instructions given by Client and acknowledged in writing by Vendor as constituting instructions for purposes of this Addendum; and (d) as reasonably necessary for the proper management and administration of Vendor's business*
- DSRs
  - *Vendor shall at its sole cost and expense promptly and in no event later than [fifteen (15)] days after Customer's request, take such actions and provide such information as Customer may request to help Customer fulfill requests of individuals to exercise their rights under Applicable Privacy Laws [defined to include CCPA], including, without limitation, requests to access, delete, opt out of the disclosure of, or receive information about the processing of, their personal information.*

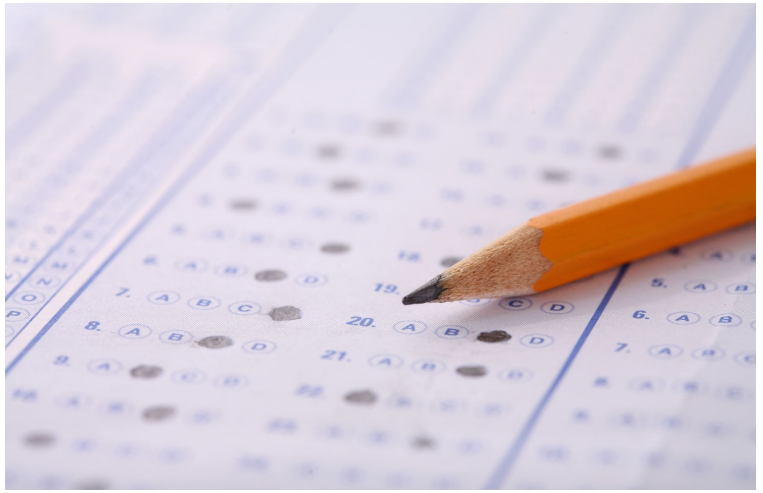
Tactical Considerations

1. Vendor Diligence Questionnaire

Cooley

Vendor Data Privacy Due Diligence Questionnaire

- A questionnaire used by organizations for collecting information externally about their vendor's privacy and data security controls. Such a tactic could be used to conduct initial due diligence or help with ongoing vendor compliance and oversight activities. A variety of sources for privacy and data security controls can be used.



Vendor Data Privacy
Due Diligence Questionnaire (cont'd)

- Vendor Business and Server Location. Please provide (a) the location of the business office(s) that will be processing Customer Data, (b) the location of all servers processing Customer Data, and (c) all non-vendor owned servers/cloud services to be used.

- EU Data Transfer Mechanism. If Vendor is located in the United States or other non-EU location, please indicate how you handle the transfer of personal data from the EU.

- Compliance with EU Directive and other data protection laws. Please describe GDPR compliance or other country-specific data protection laws.

- Data Access and Segregation. Please describe (a) who will have access to Customer Data and other Customer confidential information and (b) how Customer data PII will be segregated and secured.

Vendor Data Privacy
Due Diligence Questionnaire (cont'd)

- Privacy and Data Security Audit. Do you (a) perform a data privacy/security audits at regular intervals and (b) allow customers to audit your privacy/security procedures?

- Data Security. Please describe your security practices and how you ensure the security and confidentiality of sensitive data provided to you, and protect such information against unauthorized access or use. Do you encrypt personal information and if so, at what times and under what circumstances?

- Data Breach. Have you ever experienced a data breach involving Customer Data? If so, please detail the circumstances of the breach, its resolution, and how the conditions which allowed the breach to occur have been remedied.

- Customer Data Back-up/Disaster Recovery. Please state whether you back-up customer information/PII and how/when/where that back-up is performed.

- Sharing of Customer Data. Do you share Customer Data with any third parties? If so, please describe the circumstances under which such data may be shared.

Tactical Considerations

2. Overall Vendor Governance Checklist

Cooley

Vendor Governance Checklist

- A mechanism for organizations to document and track internally the necessary privacy and data security controls in light of the information collected, processed, and transmitted by the company.

Vendor Governance Checklist (cont'd)

- Supplier privacy policies and practices
  - Controller or Processor
  - High-risk provider - e.g., business critical, sensitive PII/PHI, or both?
- Business location(s) of:
  - Offices – e.g., service disruption potential, third part/subcontractors, etc.?
  - Servers/Systems – e.g., geographic diversity of systems, secure production environment, shadow IT, BYOD, etc.?
  - Personnel – e.g., turnover trends, training?
  - Professional service delivery – e.g., insolvency risk and data ownership/transfer?

Vendor Governance Checklist (cont'd)

- Compliance
  - Data ownership?
  - US federal and state requirements
  - EU Directive and other international requirements, country-by-country
  - Data Transfer rules per Privacy Shield, Model Clauses or Binding Corporate Rules
- Supplier network and infrastructure security policies and practices

Vendor Governance Checklist (cont'd)

- Supplier's data ecosystem and system controls:
  - Facility controls
  - System controls – e.g., thin clients, USB controls,
  - Data Controls - e.g., role based, need to know, access controls
  - Data segregation Sharing of data
  - Transmission controls – e.g., secure connectivity, encryption, redundancy
  - Documentation
- Data breach incident response
- Backup and Disaster Recovery
- Ongoing verification via independent certifications, vendor self certification or customer audit

Tactical Considerations
3. Privacy/Security Playbook

Cooley

What is a Privacy/Security Playbook?

- Guide for use when negotiating a data protection addendum or other privacy/security provisions in an agreement
- 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
- ‘Living’ document that evolves to continually 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. Service Provider must contact Customer's Privacy Office at privacy@CUSTOMER.com, the Customer's General Counsel office, or Service Provider's primary Customer contact. If Service Provider is unable to reach such contact promptly, Service Provider must again contact Customer's Privacy Office at privacy@CUSTOMER.com and provide notification that 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.	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. 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.	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).

Wrap Up and Any Other Q&A

Cooley

Recent EU Development

- New draft guidance was released on November 18, 2021 on the interplay between Article 3 of the European Union's General Data Protection Regulation (GDPR) and Chapter V of the same law.
- This new guidance specifies that personal data processing by organizations in countries outside the European Economic Area (EEA) is governed by the transfer restrictions of Chapter V, even when the organization is subject to the GDPR through the law's extraterritorial applicability. But the EDPB unhelpfully leaves open the question of how to comply with Chapter V in such circumstances, acknowledging that the required transfer tools are currently "only available in theory."

Summary points

- Privacy and security concerns have become a priority
- Legislation and litigation have caused vendor considerations to become a high priority
- Whether you are the customer or vendor, you must pay attention to clauses related to sensitive information
- Checklists or playbooks may be helpful
- Be prepared to be nimble…

Wrap up / Q & A

- Any other questions or comments?

- Thank you for your participation! Please let us know your thoughts on the session.

Cooley

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Cybersecurity and Privacy Issue-Spotting in Vendor Agreements and Standard Contractual Clauses Post Schrems and CCPA

Presented by:
Toke Vandervoort
Sandeep Kathuria
Randy V. Sabett

December 9, 2021