U.S. Businesses + GDPR

Data Processing Contracts and Vendor Management
June 26, 2018

Warner Norcross + Judd

Presenters

Norbert Kugele

Kelly Hollingsworth

The GDPR

- Legal framework for collection and processing of personal data of individuals within EU
- Came into effect May 25,2018

Who Is Subject to GDPR?

Organizations established in the EU

Organizations not established can be subject to GDPR if they:

- Offer **goods or services** to data subjects in the EU, or
- **Monitor** data subjects in the EU

Offering Goods or Services

- Applies irrespective if goods or services are free
- Is it apparent the controller ***envisages*** offering goods or services to EU data subjects?
- Website accessibility

Monitoring of Behavior

Are they being tracked?

Is data from processing being used to ***take decisions*** concerning data subject for ***analyzing/predicting*** preferences, behavior, and attitudes

Penalties & Enforceability

Penalties up to 20 million euros or 4% global revenue

Enforceability: Member country supervisory authorities & international law

Today's Focus: GDPR & 3rd Party Relationships

Relationships with vendors (processors) that have access to EU personal data need to be GDPR compliant

GDPR Basics

What/who is a data controller?

"Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"

GDPR Basics

What/who is a data processor?

"Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"

GDPR Basics

What is data processing?

"Any operation or set of operations which is performed on personal data"

GDPR Requirements Overview

Relationship governed by ***agreement*** pursuant to Article 28

If there is a cross-border transfer, data must be going into a jurisdiction with "***adequate level of protection***"

Article 24

Controller shall implement measures to ensure and demonstrate processing is GDPR compliant

Article 28: Controller-Processor Relationships

Controllers must do appropriate ***due diligence*** of vendors/processors before signing contracts.

Controllers must have ***written agreements*** with processors that must include requirements found in Article 28.

Controllers need to ***monitor*** vendors after signing contract.

Article 28:
Pre-Contract Due Diligence

"The controller shall only use processors providing ***sufficient guarantees*** that processing will meet the requirements of this Regulation"

Vendor Due Diligence

Controllers should ensure processors have sufficient guarantees re:

Expert knowledge

Reliability and resources

Technical/organizational measures that will meet GDPR

Security of processing

Article 28:
Data Processing Agreement (DPA)

"Processing by a processor shall be ***governed by a contract***...that is binding on the processor."

What Must My DPA Cover?

Subject-matter of processing

Duration of processing

Nature and purpose of processing

Type of personal data

Categories of data subjects

Obligations and rights of the controller

What Must My DPA Stipulate?

Article 28 lays out several stipulations that must be included in the DPA

What Must My DPA Stipulate?

Does my agreement cover the following?	Agreement Reference
Subject-matter of processing	
Duration of processing	
Nature and purpose of processing	
Type of personal data and categories of data subjects	
Contractual obligations and rights of the controller (e.g., indemnification, restrictions on data access, etc.)	
Does my agreement stipulate the following?	
Processor will only process data on written instructions from the controller (unless otherwise required by law)	
Processor will only transfer personal data to a third country or international organization on written instructions from the controller	
Those processing data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality	
Processor will take all measures required by Article 32 relating to security of processing	
Processor will not engage a sub-processor without prior consent from the controller	
Processor will inform controller of any intended changes regarding the addition or replacement of processors, giving the controller an opportunity to object to changes	
If the processor engages a sub-processor, they will implement the same obligations set out in the controller-processor agreement in the sub-processor agreement	
Processor is fully liable to the controller for a sub-processor's failure to fulfill data protection obligations	
Processor will assist the controller, by appropriate technical and organizational measures, in responding to data subject's rights requests	
The processor will assist the controller in ensuring compliance with Article 32 relating to security of processing	
The processor will assist the controller in ensuring compliance with Article 33 relating to notification of a data breach to a supervisory authority	
The processor will assist the controller in ensuring compliance with Article 34 relating to communication of a data breach to the data subject	
The processor will assist the controller in ensuring compliance with Article 35 relating to data protection impact assessments	
The processor will assist the controller in ensuring compliance with Article 36 relating to prior consultation with the supervisory authority	
Processor will delete or return (controller chooses) all personal data to the controller at the end of the provision of processing services	
Processor will delete existing copies of personal data at the end of the provision of processing services (unless otherwise required by law)	
Processor will make available to the controller all information necessary to demonstrate compliance with Article 28 relating to processors	
Processor will allow for and contribute to audits, including inspections, conducted by the controller or other auditors mandated by the controller	
Processor will immediately notify the controller if they believe an instruction infringes the GDPR or other Union or Member State data protections	

Continued Vendor Monitoring

Controllers are responsible for and must demonstrate compliance with Article 5(1)

Controllers are also liable for the processing of their personal data

Therefore, controllers need to make sure processors continue to be GDPR compliant to shield themselves from liability

Sub-Processors

Processors cannot engage sub-processors without prior consent/authorization from the controller

Same obligations b/t controller and processor must be imposed on sub-processor

Article 26: Joint Controllers

"Where two or more controllers jointly ***determine the purposes and means*** of processing, they shall be joint controllers."

Additional Requirements for Cross-Border Transfers

If transferring personal data outside of EU, the jurisdiction where data is going must have "***adequate level of protection***"

Protection isn't referring to security, but the protections afforded by law re: data

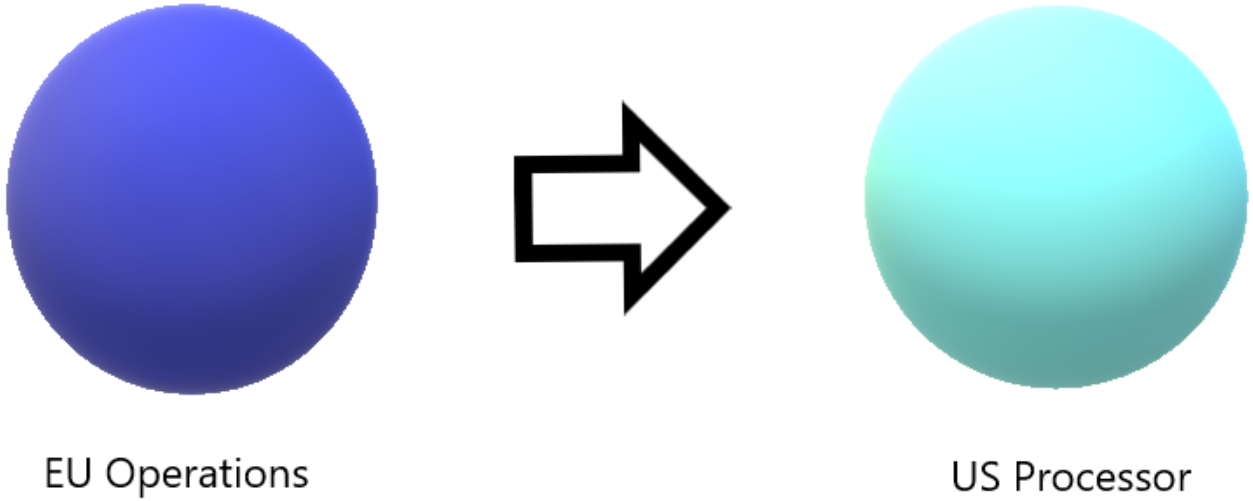
If no adequate level of protection, you need something more than a DPA

Article 46

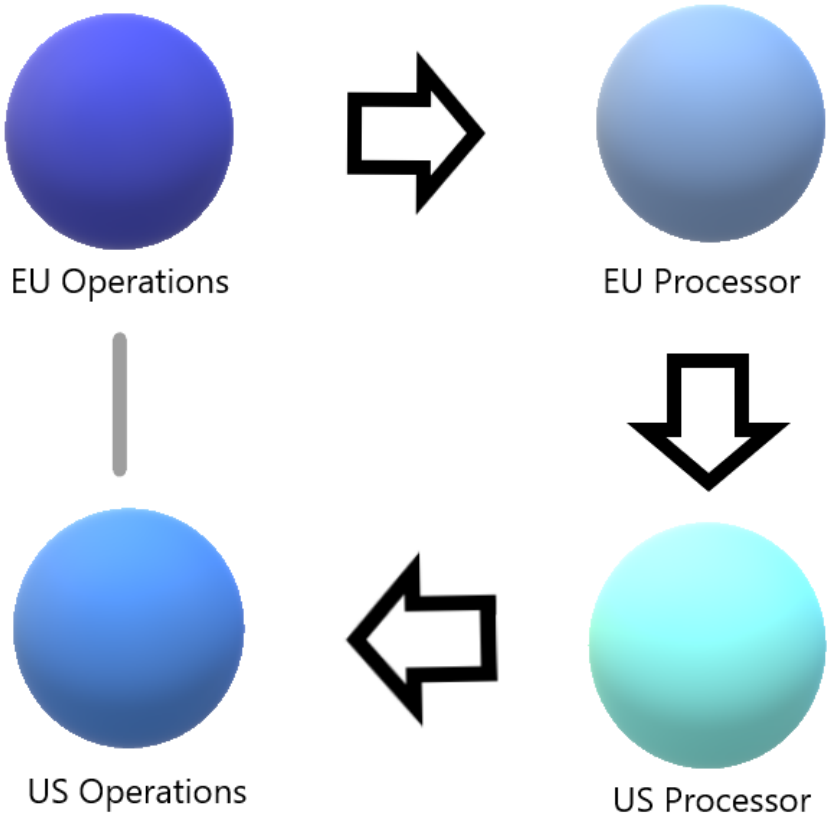
If no adequacy decision, transfer may only happen if controller/processor has provided "***appropriate safeguards***"

Scenario 1

Scenario 2



Scenario 3



Takeaways

1. Controllers have vendor relationship responsibilities before, at and after contracting
2. Vendor relationships NEED written agreements
3. Cross-border transfers have additional requirements

Questions?

Thank you!

Norbert Kugele: nkugele@wnj.com

Kelly Hollingsworth: khollingsworth@wnj.com

Warner Norcross + Judd