WSGR Getting Ready for the GDPR Series

Session 3: The GDPR for Service Providers

Cédric Burton
Of Counsel

Laura De Boel
Senior Associate

Agenda

- Introduction.
- Current rules for service providers under EU data protection law.
- New rules under the EU General Data Protection Regulation (GDPR):
  - Statutory obligations.
  - Contractual obligations.
  - Indirect impact on service providers.
- Conclusions.
- Q&As.

Introduction

- Service providers acting as processors have limited obligations under current EU Data Protection Directive.
- This will change as of May 25, 2018, when the EU General Data Protection Regulation (GDPR) becomes effective and replaces the Data Protection Directive.
- The GDPR is a game-changer. It will significantly affect service providers:
  - Even if no establishment in the EU but processing EU data (extraterritorial effect).
  - A number of GDPR provisions are explicitly and directly addressed to processors.
  - The GDPR mandates a large number of contractual provisions.
  - As a result, burden of compliance increases for processors.
  - Civil liability and risk of fines of up to 4% of annual worldwide turnover.
- One of the most important changes introduced by the GDPR.

Start preparing now! Follow our WSGR Getting ready for the GDPR series

International data transfers under the GDPR.	**September**
Regulatory aspects of the GDPR: DPAs' powers, EDPB, one-stop shop, recourse mechanisms.	October
Panel discussion with leading privacy officers on how to get ready for the GDPR.	November

Current Rules

- Controller vs. Processor: Different roles and responsibilities.

Controller	Processor
Entity that, alone or jointly with others, determines purposes (“why”) and means (“how”) of data processing.	Entity that processes personal data on behalf of and under instructions of controller.
Example: EU customers.	Example: Cloud service providers.

- The burden of compliance with EU data protection law lies with controllers.
- Service providers acting as processors must be bound by a written data processing agreement that requires them to (1) comply with controller’s instructions; and (2) implement appropriate security and confidentiality measures.
- The GDPR maintains these concepts but significantly increases the compliance burden on data processors.

The GDPR for Service Providers in a Nutshell

- Controllers are required to seek sufficient guarantees from processors.
- Imposes several direct obligations on processors.
- Mandates new provisions for data processing agreements.
- Requires processors to cooperate with and assist their customers.
- Focuses on ensuring the protection of individuals rights.
- Increases duty of due diligence for controllers when selecting processors.
- Introduces possibility for individuals to claim compensation from the processor if they suffered damage and the processor:
  - Didn't comply with the GDPR obligations specifically directed to processors; or
  - Acted outside or contrary to lawful instructions of the controller.
- Introduces possibility for DPAs to impose administrative fines of up to 4% of total worldwide annual turnover on processors.

Three Categories of Changes

1. **Direct statutory obligations.** The GDPR imposes direct obligations on processors:
   - Paradigm shift.
2. **Contractual obligations.** The GDPR imposes on controllers a prescriptive list of clauses for data processing agreements:
   - Significant impact on your contract management.
3. **Indirect impact on processors.** The GDPR obligations addressed to controllers will indirectly impact processors:
   - Enable controllers to comply with their obligations.

Statutory Obligations

Does the GDPR Directly Apply to You?

- Material scope:
  - Data processors processing personal data.
- Territorial scope:
  - When data processors are established in the EU:
    - Irrelevant whether the processing takes place in the EU.
  - When data processors are not established in the EU, and the processing involves data of individuals located in the EU, if the processing is related to either:
    - The offering of goods or services to individuals located in the EU (even free of charge); or
    - The monitoring of their behavior.
- Data processors without EU establishment must appoint a representative in the EU.

Security Measures

- Data processors must implement *appropriate* technical and organizational measures to protect the data.
- Protect from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data processed.
- What is appropriate depends on:
  - State of the art;
  - Costs of implementation; and
  - Risks related to processing (depending on nature, scope, context and purposes of processing, and risk for rights and freedoms).
- Security measures should, as appropriate:
  - Include pseudonymization and encryption of data;
  - Ensure the confidentiality, integrity, availability and resilience of processing systems;
  - Allow to restore the availability and access to data in a timely manner following a technical incident;
  - Entail a process for regularly testing, assessing and evaluating the effectiveness of the security measures.
- Possibility to demonstrate compliance by adhering to an approved code of conduct / certification mechanism (not available at EU level yet).
- Any individual accessing personal data must be bound by confidentiality obligations.

Other Obligations (1)

- Cooperation obligation:
  - Help controllers comply with their obligations regarding (i) data security, (ii) privacy impact assessments, (iii) data breach notification, and (iv) prior consultation with DPA.
  - Details of cooperation and assistance must be included in data processing agreements.
- Records:
  - Maintain records of processing activities to demonstrate compliance with GDPR.
  - Prescriptive content (e.g., data transfers; security measures).
  - Must be available to DPAs upon their request.
  - Exemption: less than 250 employees (unless sensitive data are processed; the processing is likely to result in high risks; or the processing is repetitive).
- DPO:
  - Obligation to appoint a DPO if sensitive data are processed on a large scale or the core processing activities require monitoring of individuals on a large scale.

Other Obligations (2)

- Data breach notification to customers:
  - Notify the customer of a data breach; not individuals or the DPA.
  - Without undue delay after becoming aware of the data breach.
- Comply with data transfer restrictions:
  - Direct obligation is major shift from current Data Protection Directive.
  - Applies to initial transfer and onward transfers.
  - Applies in addition to the obligation to act on behalf of and under instructions of controller.
  - We will likely see new data transfer mechanisms for processors such as P2P clauses.
  - Possibility to adhere to approved codes of conduct and certification mechanisms for companies established outside the EU (not available yet).

Contractual Obligations

Data Processing Agreement / Clauses (1)

- Under Data Protection Directive, the provisions explicitly required by law were limited to: (i) only act on instructions from the controller; and (ii) ensure appropriate security measures.
- The GDPR introduces a large number of mandatory provisions to include in data processing agreements.
- The GDPR requires description of:
  - Subject-matter of processing;
  - Duration of processing;
  - Nature and purposes of processing;
  - Types of personal data and categories of individuals.

  ⇨ Expect descriptions similar to Appendix 1 to EU Controller–to–Processor Model Contract.
- The roles and responsibilities of both controller and processor must be clearly defined in written data processing agreements.
- If a processor receives unlawful instruction from the controller, it must inform the controller.

Data Processing Agreement / Clauses (2)

Obligations of the processor in contract	Directive	GDPR
Process data only on documented instructions from the controller, including regarding international data transfers	✓ (less specific)	✓
Ensure that persons authorized to process data are bound by confidentiality requirements	N/A	✓
Take all security measures appropriate to the risks of the processing	✓ (less specific)	✓
Comply with sub-contracting restrictions	N/A	✓
Take appropriate technical and organizational measures, insofar as possible, to fulfil controller's obligation to respond to individuals' requests	N/A	✓
Assist the controller in ensuring its compliance with security requirements; data breach notification requirement; PIAs; and prior consultation with DPA	N/A	✓
Delete or return all data to the controller, at the choice of the controller. To delete all copies, unless EU or national law requires the processor to store such data	N/A	✓
Make available to the controller all information necessary to demonstrate compliance	N/A	✓
Allow for and contribute to audits, including inspections, conducted by the controller or another auditor	N/A	✓

Sub-contracting

Mandatory prior written authorization of the controller

specific

- No sub-processing without opt-in consent.

or

general

- Obligation to inform the controller of any planned changes to the sub-processors.
- The controller is entitled to object to such changes.

- General authorization is more flexible.
- Consider creation of tool to update list of sub-processors and to keep customers informed.
- Obligation to impose same data protection obligations on sub-processor as are imposed on processor by way of a sub-processing agreement.

Impact on Your Contract Management

- Significant impact on contract management:
  - Consider preparing or updating template agreements:
    - GDPR requirements are largely based on German requirements for data processing agreements and the EU Controller-to-Processor Model Contract.
    - Option to use standard contractual clauses adopted by EU Commission or national DPA (not available yet).
  - Controllers and processors need to review existing agreements.
  - Probably one of the most time & resource consuming aspects of the GDPR!
    - Need to allocate time and resources to contract management team.

Indirect Impact

Indirect Impact on Processors

- Beside the statutory and contractual requirements, processors should enable controllers to comply with their own obligations under the GDPR as a business proposition.
- Areas in which this may be particularly relevant:
  - Responding to individuals who exercise their data protection rights (e.g., data portability right, right to erasure – also called “the right to be forgotten”).
  - Embedding privacy-by-design and privacy-by-default into services.
    - Build products and services in a way that allows controllers to comply with new obligations.
  - Implementing strong data breach notification process.
  - Implementing process for responding to data access requests from authorities.
  - Conducting Privacy Impact Assessment.

Conclusions

- The GDPR significantly increases obligations on service providers acting as processors.
- Although the GDPR imposes strict obligations, it also introduces new ways to demonstrate compliance, such as adherence to approved codes of conduct and certification mechanisms.
- The GDPR is a game-changer; enforcement risk for processors will be much higher.
- Use the 2-year transition period wisely:
  - Understand your obligations.
  - Modify your processes and contracts.
  - Make GDPR compliance your asset.
- **Stay tuned for our next webcasts!**

International data transfers under the GDPR	**September**
Regulatory aspects of the GDPR: DPAs' powers, the EDPB, the one-stop shop, recourse mechanisms	October
A panel discussion with leading privacy officers on how to get ready for the GDPR	November

Questions?

Thanks!

Cédric Burton
Of Counsel
cburton@wsgr.com

Laura De Boel
Senior Associate
ldeboel@wsgr.com

WSGR Regulation Observatory:
www.wsgr.com/EUDataRegulation

WSGR resources

- WSGR EU Data Protection Observatory (with full background information and analysis of the GDPR, legislative texts, and all articles cited below): www.wsgr.com/EUDataRegulation.
- WSGR Data Advisor: www.wsgrdataadvisor.com.
- C. Burton, L. De Boel, S. Cadiot and S. Hoffman, *New EU Data Protection Regulation Is Now Enacted*, WSGR Alert, April 14, 2016.
- C. Burton, L. De Boel, C. Kuner, S. Cadiot and S. Hoffman, *The Final European Union General Data Protection Regulation*, BNA, January 25, 2016.
- C. Burton, L. De Boel, C. Kuner, A. Pateraki, *The Proposed EU Data Protection Regulation Three Years Later: The Council Position*, BNA June 29, 2015.
- C. Burton, C. Kuner, A. Pateraki, *The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report*, BNA, January 21, 2013.
- C. Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, BNA, February 6, 2012.