WSGR Getting Ready for the GDPR Series

Session 5:
Regulatory Aspects of the GDPR

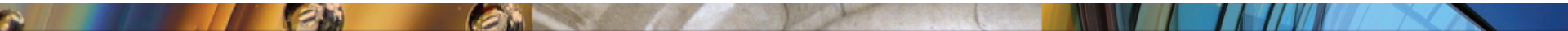
Cédric Burton
Of Counsel

Laura De Boel
Senior Associate

Christopher Kuner
Senior Privacy Counsel

WSGR Webcast, Brussels, November 17, 2016

Wilson Sonsini Goodrich & Rosati, LLP



Agenda

- Introduction.
- Current rules v. GDPR rules.
- Enforcement powers.
- Increased judicial remedies.
- The One-Stop Shop.
- Cooperation mechanism.
- Consistency mechanism.
- Imaginary case study.
- Questions & Answers.

What's new under the GDPR?

- One-stop shop: companies processing data in multiple EU countries will deal with one lead Data Protection Authority (DPA).
- Cooperation procedure and consistency mechanisms:
  - To facilitate cooperation among DPAs; and
  - To ensure consistency in GDPR application and enforcement.
- European Data Protection Board (EDPB):
  - Replaces Article 29 Working Party (WP29).
  - More formal and regulated body with power to issue binding decisions.
- Increased and harmonized powers for DPAs.
- High fines: up to 20 million EUR or 4 percent of worldwide turnover.
- DPAs' resources will likely increase.
- Expect strengthened enforcement.
- Learning experience for DPAs. DPAs are currently working on how mechanics will work in practice.

Current rules v. GDPR rules

Topic	Current rules	GDPR
Regulatory fragmentation	Companies deal with DPAs in each EU country in which they process personal data: • 28 EU countries, some of which have more than one DPA (e.g., Germany). • Significant administrative burden. • Fragmentation due to inconsistent approaches of DPAs and national courts.	GDPR aims to remedy fragmentation: • One-stop shop mechanism: for cross-border data processing activities, companies will deal with one DPA ("lead DPA"). • Consistency mechanism ensures harmonized application of GDPR.
Central regulatory body	WP29: • Assembly of national DPAs. • While quite influential, its powers are limited to issuing non-binding opinions and recommendations.	EDPB: • Will replace WP29. • More institutionalized than WP29. • With power to issue binding decisions.
Enforcement	Fragmented enforcement: • National DPAs have different powers, and some cannot impose fines on companies. • Relatively low fines.	Harmonized enforcement: • Harmonized powers of DPAs. • Introduction of massive fines of up to 20,000,000 EUR or 4% of annual worldwide turnover.

Robust enforcement powers

- Main risk was reputational risk, but enforcement is significantly increasing.
- GDPR is a game-changer: strong DPAs' powers, judicial remedies, and increased fines.

DPAs' investigative powers	• Order companies to provide any information needed to perform their tasks. • Notify companies in case of infringement. • Conduct investigations (e.g., data protection audits). • **Dawn raids.**
DPAs' corrective powers	• Issue warnings or reprimands. • Order companies to comply with individuals' rights. • Order companies to bring processing activities in compliance with GDPR. • **Impose limitation, including a ban, on processing.** • **Suspend data transfers.** • Order companies to inform individuals of a data breach. • **Impose massive fines (two-tiered system: up to 10,000,000 EUR or 2% of global turnover, whichever is higher; or up to 20,000,000 EUR or 4%).**
DPAs' authorization and advisory powers	• Prior consultation. • Opinion and approval of draft codes of conduct. • Accreditation of certification bodies. • Adoption of standard data processing agreements and standard sub-processing agreements. • Adoption of SCC and authorization of *ad hoc* data transfer clauses. • Approval of BCRs.

Fines

- Introduction of two-tiered system of administrative fines.
- DPAs can impose fines also on processors for breach of the GDPR provisions directed to them.

Up to 10,000,000 EUR or 2% of global turnover, whichever is higher	**Up to 20,000,000 EUR or 4% of global turnover, whichever is higher**
For non-compliance with the requirements on, e.g.: • Internal records of processing activities • Cooperation with a DPA upon its request • Privacy by Design or Privacy by Default • Security • Data breach notification	For non-compliance with, e.g.: • Core data protection principles • Individuals' rights • Consent requirements (i.e., for not being able to demonstrate that the individual has consented to the processing) • Data transfer restrictions • DPA's orders

Increased judicial remedies

- Increased remedies for individuals:
  - Right to complain to a DPA (to be included in privacy notice).
  - Right to challenge DPA's decision before courts.
  - Right to obtain an effective judicial remedy against a controller or a processor.
  - Right to seek compensation for damages against a controller or a processor.
- Privacy NGOs:
  - Can file complaints on behalf of individuals and represent individuals before courts.
  - Can seek remedies (except for compensation) independently of individual's mandate only if national law allows.
- Same rights to remedies in all EU countries.

From a true one-stop shop to a complex mechanism

- Commission proposal: one-stop shop DPA for companies and individuals.
- Negotiations and political compromises substantially modified proposal.
  - One-stop shop would be less protective for individuals (e.g., need to lodge complaint in foreign country, in different language).
  - Political discussions.
- Result is a complex mechanism to deal with cross-border cases and ensure consistent application and enforcement of EU law.
  - Applies in cross-border cases when multiple DPAs are involved in same matter or where individuals from multiple countries are affected by the processing activities.
  - One contact point for cross-border matters.
  - Application to non-EU controllers and processors without EU establishment is unclear.
  - Lead DPA is DPA of EU country where company has its main establishment.
  - Individuals can lodge complaint with local DPA who will channel it to the company's lead DPA:
    - In principle, local DPA adopts decision regarding individual, lead DPA regarding company.
    - If matter is purely local, local DPA may deal with it entirely (unless lead DPA disagrees).
  - All DPAs concerned cooperate with lead DPA to reach final decision:
    - EDPB deals with DPAs' disagreements (consistency mechanism).

Main establishment

- Main establishment is where company has central administration in EU.
  - CJEU case-law clarified concept of ‘establishment’: effective and real exercise of activity through stable arrangements *(Weltimmo).*
  - No definition of ‘central administration’.
  - Company’s legal form does not determine main establishment.
  - Location of servers used for data processing is not decisive.
- Exceptions:
  - Controller: if decisions on purposes and means of processing are taken in other EU establishment (which has the power to implement them).
  - Processor: if no central administration in EU, establishment in country where main processing activities take place.
- In cases involving both controller and processor, lead DPA is DPA of controller (with some involvement from lead DPA of processor).
- If DPAs disagree, EDPB can decide which DPA is the lead DPA.
- Document objective justifications for choice of main establishment.

Representative in EU

- No establishment in EU?
- Obligation to designate representative in EU:
  - Natural or legal person designated in writing.
  - Established in one of the EU countries where individuals whose personal data are processed are located.
  - Represents company re: its obligations under GDPR:
    - Individuals and DPAs can address representative in addition to or instead of company.
    - DPAs can enforce against representative.
  - Legal actions can be initiated against company, even if representative has been designated (no change of liability).
  - Exemption from the obligation to appoint representative: occasional processing that does not include sensitive data, and which is unlikely to result in high risks for individuals.

Cooperation mechanism

- Mechanism that allows lead DPA and DPAs concerned to cooperate on cross-border case.
  - 'DPA concerned' is:
    - DPA of EU country where controller or processor is established.
    - DPA of EU country whose individuals are (likely to be) substantially affected.
    - DPA with which complaint was lodged.
- To which cases does it apply?
  - Cases involving cross-border processing.
  - Local cases, where lead DPA requests to handle them.
- How does it work?
  - Lead DPA sends draft decision to DPAs concerned.
  - There are three scenarios:

(1) Consensus	(2) DPA objects and lead DPA agrees	(3) DPA objects and lead DPA disagrees: consistency mechanism
• DPAs concerned agree with draft decision.	• Lead DPA revises draft decision in accordance with objection and submits revised decision to all DPAs concerned.	• Consistency mechanism is triggered either when lead DPA (i) does not intend to follow objection; or (ii) considers that objection is "not relevant or reasoned".

Consistency mechanism

- Mechanism aimed at ensuring a consistent application and enforcement of EU data protection law.
- EDPB acts as the arbitrator of disputes via binding decisions or opinions.
- Consistency mechanism is triggered in different scenarios:
  - Binding decisions:
    - Disagreement among DPAs in the context of the cooperation mechanism.
    - Dispute re: which DPA is lead DPA.
    - DPA does not request mandatory opinion of EDPB, or does not follow EDPB opinion.
  - Opinions:
    - DPAs must request opinion from EDPB before adopting certain measures specified in GDPR, e.g.:
      - List of data processing activities that require Privacy Impact Assessment.
      - Approval of Binding Corporate Rules.
    - EDPB must opine on any matter of general application / producing effects in more than one EU country, if requested by EU Commission, Chair of EDPB, or any DPA.

Urgency procedure, mutual assistance and joint operations

- Urgency procedure:
  - Exception to cooperation or consistency mechanisms.
  - When urgency requires immediate measures, with involvement of EDPB.
- DPAs must provide each other with mutual assistance, e.g.:
  - Information requests.
  - Supervisory measures (e.g., requests to carry out prior consultations).
- DPAs are able to conduct joint operations “where appropriate”, e.g.:
  - Joint investigations.
  - Joint enforcement measures.
  - Monitoring implementation of measure imposed on company established in another EU country.

How to challenge EDPB and DPA's decisions

- EDPB and DPA's decisions can be challenged before different courts.
- EDPB: before CJEU.
  - Bring action for annulment of EDPB decision before CJEU.
  - Limited conditions in which action can be brought (Art. 263 TFEU).
  - Only DPA to whom EDPB decision is addressed and those who are (individually and directly) concerned by EDPB decision can bring action.
  - Within two months following publication of EDPB decision on EDPB website.
  - Lengthy procedure before CJEU.
- DPA's: before national courts.
  - Challenge DPA's decision before national courts of DPA's country, under procedural law of that country.
  - National courts exercise full jurisdiction and examine all questions of fact and law.
  - National courts may always ask CJEU how to interpret EU law.
  - If DPA's decision implementing EDPB decision is challenged, and national court considers EDPB decision to be invalid, CJEU must rule on validity.

Imaginary case study

- Facts:
  - "Waffle SA" has HQ in Belgium, and establishments in France, Germany, Italy, Poland and Spain.
  - Lead DPA is Belgian DPA.
  - French individual files complaint against Waffle with French DPA.
- Cooperation procedure:
  - French DPA must inform Belgian DPA.
  - Belgian DPA determines it is cross-border matter and decides to handle case.
  - Belgian DPA submits draft decision to all DPAs concerned (i.e., French, German, Italian, Polish and Spanish).
  - French DPA objects, others agree.
  - Belgian DPA stands by its draft decision. This triggers consistency mechanism.
- Consistency mechanism:
  - EDPB confirms Belgian DPA's decision. Binding on Belgian DPA and all DPAs concerned.
  - Belgian DPA issues its decision to fine Waffle. French DPA informs complainant on decision.
- Waffle's options:
  - Request annulment of EDPB decision before CJEU (within 2 months).
  - Challenge Belgian DPA's decision before Belgian courts / tribunals in accordance with Belgian procedural law.

Open questions & outlook

- A number of questions remain open, e.g.:
  - One-stop shop mechanism:
    - Uncertainty for non-EU controllers and processors without establishment in EU.
    - Would representative be considered to be main establishment?
  - Fines:
    - What is “total worldwide annual turnover of the preceding financial year”?
    - Turnover of EU entity, non-EU entity, or entire group?
    - Uncertainty re who will fine: one fine by DPA or several fines by all DPAs concerned?
- Outlook:
  - GDPR will change regulatory landscape, but how and if the one-stop shop and complementing mechanisms will work in practice remains to be seen. Efficiency will be tested in practice.
  - In any case, expect strengthened enforcement.
  - Establish good relationship with lead DPA.
  - Keep monitoring developments!

Questions?

Thank you!

Cédric Burton
Of Counsel
cburton@wsgr.com

Laura De Boel
Senior Associate
ldeboel@wsgr.com

Christopher Kuner
Senior Privacy Counsel
ckuner@wsgr.com

Twitter: @EUDataPrivacy

GDPR Observatory: www.wsgr.com/eudataregulation/

WSGR Resources

- WSGR Data Advisor: www.wsgrdataadvisor.com
- WSGR EU Data Protection Observatory: www.wsgr.com/EUDataRegulation
- Articles:
  - C. Burton, S. Cadiot, L. De Boel, S. Hoffman, "Article 29 Working Party Issues Statement Following Adoption of EU-U.S. Privacy Shield", WSGR Alert, July 26, 2016
  - C. Burton, S. Cadiot, L. De Boel, S. Hoffman, "The EU-U.S. Privacy Shield Is Adopted and Available as of August 1, 2016", WSGR Alert, July 12, 2016
  - C. Kuner, C. Burton, S. Cadiot, S. Hoffman, L. De Boel, "Uncertainty Increases Around EU-U.S. Data Flows", WSGR Alert, May 26, 2016
  - C. Kuner, C. Burton, L. De Boel, S. Hoffman, S. Cadiot, "New EU Data Protection Regulation Is Now Enacted", WSGR Alert, April 14, 2016
  - C. Kuner, C. Burton, L. De Boel, S. Cadiot, S. Hoffman, "EU Commission Publishes EU-U.S. Privacy Shield," WSGR Alert, February 29, 2016