
Morgan Lewis
TECHNOLOGY MAY-RATHON
WHAT DO TECHNOLOGY BUSINESSES NEED TO KNOW ABOUT THE GDPR?
Ron Del Sesto, Pulina Whitaker, Dr. Axel Spies
May 22, 2017
© 2017 Morgan, Lewis & Bockius LLP

Agenda

- The New EU General Data Protection Regulation
- Controller and Processor Obligations Under the GDPR
- Cross-Border Transfers of Personal Data—Privacy Shield Update
- Q&A

SECTION 01

THE NEW EU GENERAL DATA PROTECTION REGULATION OR GDPR

The New EU General Data Protection Regulation

- New GDPR will replace existing EU Data Protection Directive for commercial data privacy obligations starting 25 May 2018
- “Personal Data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person
- Personal data still to be processed fairly and lawfully
- Pseudonymisation/anonymisation distinction
- Consent
  - explicit
  - freely given
  - fully informed

The New EU General Data Protection Regulation, cont'd

- International transfers: Binding Corporate Rules, model clauses, to certified organization, consent, transfer is "necessary" for performance of contract, establish, exercise or defend legal claims or for legitimate interests of controller (one-off and limited data subjects involved), adequate countries
- Data Protection Officer: for controllers/processors processing substantial sensitive personal data or who have core activity of monitoring individuals on a large scale or public body
- Right to request to be forgotten, have data rectified or deleted
- Privacy by design: privacy safeguarding technology built-in from the start
- Actively factor privacy considerations into the design and upgrade of all systems, policies, settings which process personal data
- Privacy by default: privacy-friendly default settings until user chooses otherwise

The New EU General Data Protection Regulation, cont'd

- Data protection impact assessment: prior to processing if high risk for individuals
- Notify data breach to DPA without undue delay/within 72 hours and to individuals without undue delay if there is likely to be high risk to individuals
- Most EU countries currently limit data protection breaches to around £500,000 per breach – average is £100,000
- Penalties for breach of GDPR – up to higher of 4% global turnover or €20,000,000
- Controllers and processors will be directly liable under GDPR

The New EU General Data Protection Regulation, cont'd

- Expanded application of the EU data privacy obligations
- The GDPR will apply to processors and controllers having an EU-based establishment where personal data are processed in the context of the activities of this establishment
- The GDPR will also apply to controllers and processors based outside the EU territory where the processing of personal data regarding EU data subjects relates to:
    - the offering of goods or services (regardless of payment)
    - the monitoring of data subjects' behavior within the EU

SECTION 02

CONTROLLER AND PROCESSOR OBLIGATIONS UNDER THE GDPR

Definitions of Controller, Processor and Processing

"**Controller**" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.

"**Processor**" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

"**Processing**" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controllers Must Ensure the Processing of Personal Data Complies with Certain Principles

1. **Lawfulness, fairness and transparency** – Imposes a disclosure obligation such that data subjects are informed as to what their personal data will be used for;
2. **Purpose limitation** - Personal data must be collected only for an explicit purpose and not subject to additional processing that would be inconsistent with the specified purpose;
3. **Data minimization** - Only process personal data actually needed to achieve stated purpose;
4. **Accuracy** - Personal data must be accurate and kept up to date. Inaccurate personal data should be corrected or deleted;
5. **Retention** – Stored for no longer than is necessary to achieve the processing purpose;
6. **Data Security**- Covered later in the presentation; and
7. **Accountability** – Must be able to demonstrate compliance with data protection obligations.

Using Third Party Data Processors

- Where processing is to be carried out on behalf of a controller, the controller **shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures**.

- The processor shall not engage another processor (sub-processors) without **prior specific or general written authorization of the controller**. In the case of general written authorization, the processor **shall inform the controller of any intended changes** concerning the addition or replacement of other processors, thereby **giving the controller the opportunity to object to such changes**.

Selected Processor Obligations

1. Processor must not appoint a sub-processor **without the prior written consent of the controller**. Sub-processors must be subject to flow-down obligations from the processor.
2. Processor is subject to confidentiality obligations and personnel must have same.
3. Processors (and any sub-processors) shall not process personal data, except in accordance with the instructions of the controller, or the requirements of EU law or the national laws of Member States.
4. Recordkeeping obligations
5. Cooperate with Data Protection Authorities
6. Data Security Obligations
7. Data breach reporting
8. Appointment of a Data Protection Officer (if applicable)
9. Cross border Transfers

Controller and Processor Data Security Obligations

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk associated with the nature of the personal data collected, the controller and the processor must implement "**appropriate technical and organizational measures**" to ensure a level of security appropriate to the risk which may include:

1. Pseudonymisation/Encryption of Personal Data;
2. Business continuity (backup and redundancy);
3. Regularly assessing, evaluating and testing of such technical and organizational measures; and
4. Data breach notification obligations

Adherence to an approved Code of Conduct may provide evidence that the controller and processor have satisfied these obligations.

Data Processor Contracts: Mandatory Provisions

1. Scope, nature and purpose of processing must be defined;
2. Identify types of personal data to be processed;
3. Duration of the processing;
4. Processes the personal data only on documented instructions from the controller;
5. Data security obligations must be addressed;
6. Processor must assist controller in meeting its obligations regarding data breaches;

Data Processor Contracts: Mandatory Provisions (cont'd)

7. Processor must assist controller in satisfying requests from data subjects;
8. Processor must return or delete personal data at end of contract;
9. Demonstrate compliance with all of the obligations imposed by the GDPR;
10. Allow the controller to perform compliance audits;
11. Consent of the controller is required if processor uses a sub-processor;
12. Flow-down obligations imposed on sub-processor; and
13. Independent obligation to inform the controller if, in its opinion, the controller's instructions would breach Union or Member State law

Joint Liability

Article 26(3)

The data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 82

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

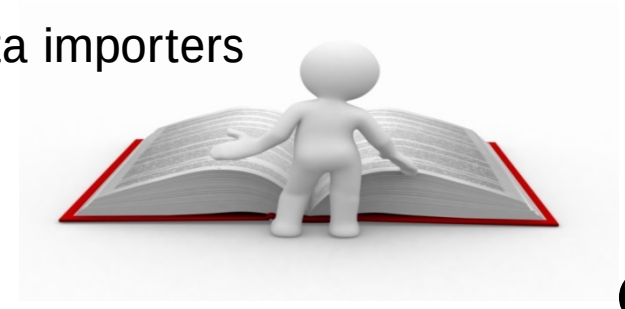
SECTION 03

GDPR AND GERMANY

CROSS-BORDER TRANSFERS OF PERSONAL DATA—PRIVACY SHIELD UPDATE

EU-U.S. Privacy Shield (PS) – What Is It?

- Necessary because of European Court of Justice's (ECJ's) "Schrems" decision of Oct. 6, 2015 (C-362/14), striking down EU-U.S. "Safe Harbor"
- Available since August 1, 2016 – PS Framework
- Voluntary – U.S. data importers can self-testify with U.S. Department of Commerce
- Covers many, but not all, EU-U.S. data flows
- Enforced by FTC/DOT
- Public PS register with statements of approved data importers
- Complicated dispute resolution mechanism



EU-U.S. Privacy Shield (PS) – How Safe Is It?

- PS is **not** based on an international treaty
- U.S. Secretary **Ross** recently stated that the Trump administration will honor the PS commitments of the Obama administration

Legal Risks:

- EU concerns about access to PS data by U.S. authorities remain
- U.S. visit of EU Commissioner Jourová (Justice)
- Joint annual review process of PS (U.S. surveillance) in September
- Pending legal case at ECJ
- New legal challenge of Schrems in Ireland (referral to the ECJ?)

PS compliance remains challenging:

- How to ensure that onward transfers of PS data are/remain in
- compliance?

EU Data Transfers

- Current alternatives
  - “Derogations” e.g. consent to transfer outside the EU or “necessary” transfers to comply with contractual obligations or litigation management
  - Standard Contractual Clauses
  - Binding Corporate Rules
  - Assessment of adequacy
- Under the GDPR, additional options of:
  - Code of Conduct
  - Certification of mechanism and privacy seals and marks
  - Binding Corporate Rules extended to processors

Germany: GDPR Implemented by Separate Law, the DSAnpUG -EU

- New German implementation law (DSAnpUG-EU)
  - Will not abrogate, but amend the German Federal Data Protection Act (BDSG)
  - 85 Articles of the new BDSG: the current BDSG has 48!
  - Detailed new Sec. 26 BDSG on HR-data
    - New definition of "employee" ⟷ "data subject"
    - "Managers" of German companies may be exempted.
  - Does Sec. 26 BDSG (new) comply with Art. 88 GDPR?
  - New lengthy "German" definition of sensitive data in Sec. 22 BDSG (new)
  - National exemptions for disclosure requirements
  - No time for an intensive legal discussion

DSAnpUG - Consequences

- The optimistic statement that the GDPR will bring about the same standards of data protection throughout the EU is wishful thinking.
- DSAnpUG will also have an impact on the national requirements for consents and for the disclosure requirements
- Other EU members states looking for guidance

Q&A

Thank you for joining this event in our Technology May-rathon series.

We would be pleased to answer your questions.

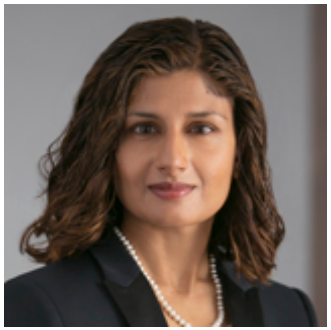
The Q&A tab is located on the bottom right hand side of your screen. Please type your questions in the space provided and click Send.

Biography

Ronald W. Del Sesto, Jr.
Washington, DC
T +1.202.373.6023
E ronald.delsesto@morganlewis.com

Ronald W. Del Sesto, Jr. is a partner in the telecommunications, media, and technology (TMT) practice group. Ron's practice concentrates on the representation of technology companies on a broad range of issues including corporate, financial, regulatory, and cybersecurity. Ron also advises financial institutions, private equity firms, and venture capital funds with respect to investments in the TMT sectors.

Biography



Pulina Whitaker

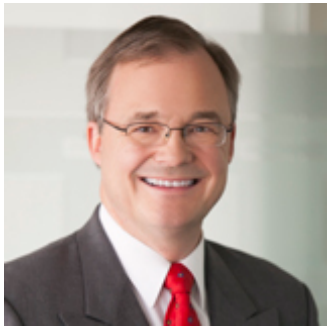
London

T +44.20.3201.5550

E pulina.whitaker@morganlewis.com

Pulina Whitaker focuses her practice on a variety of data privacy and data protection matters, including advising on international transfers of personal data, third-party transfers, data breach investigations and rights of access to personal data. She also advises on setting-up whistleblower hotlines for European-based companies and compliance with Sarbanes-Oxley Act requirements and other international investigations and compliance matters.

Biography



Dr. Axel Spies advises domestic and international clients on various international issues, including licensing, competition, corporate issues, and new technologies. He counsels on international data transfers, privacy, technology licensing, EU sanctions, e-discovery, and equity purchases. A member of the Sedona Conference on Electronic Discovery with a focus on German and international data protection, Dr. Spies is frequently quoted for his telecommunications and privacy knowledge and co-publisher of the ZD (data protection journal) and MMR (Multi-Media Law) in Germany.

Dr. Axel Spies

Washington, DC

T + 1.202.739.6145

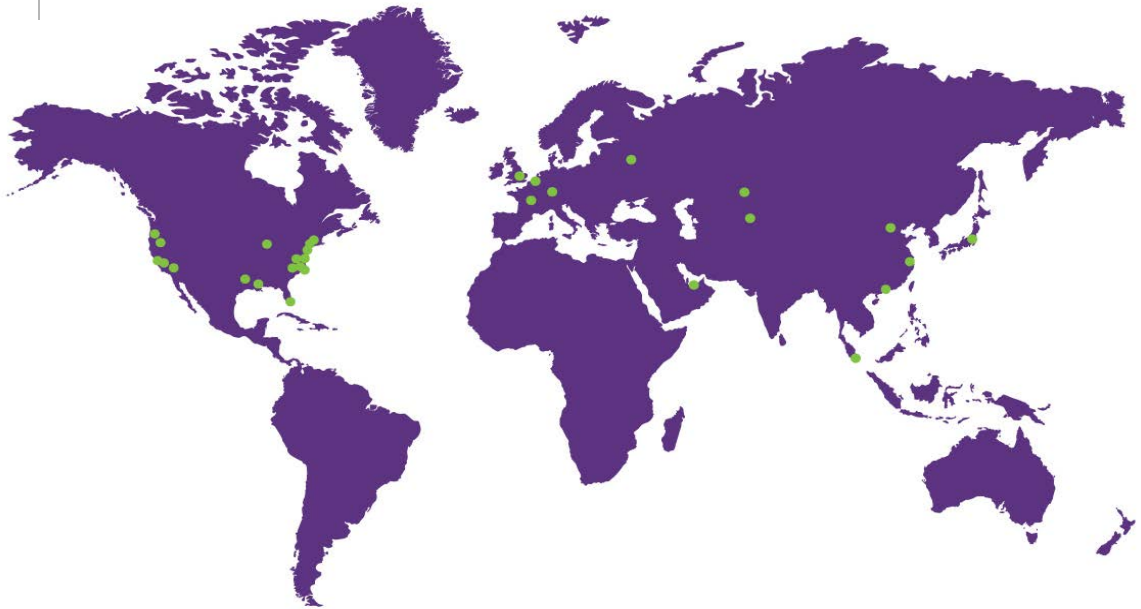
E axel.spies@morganlewis.com

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing*
Boston
Brussels
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Santa Monica
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing office operates as a representative office of Morgan, Lewis & Bockius LLP. In Shanghai, we operate as a branch of Morgan Lewis Consulting (Beijing) Company Limited, and an application to establish a representative office of the firm is pending before the Ministry of Justice. In Hong Kong, Morgan Lewis has filed an application to become a registered foreign law firm and is seeking approval with The Law Society of Hong Kong to associate with Luk & Partners.

THANK YOU