THE GDPR: WHAT HR NEEDS TO KNOW

March 29, 2017

people doc

Introductions

Top Global Data Privacy Lawyers

Arnaud Gouachon
Chief Legal &
Compliance Officer

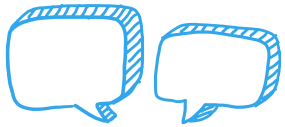
Ezra D. Church
Partner
Morgan Lewis

Pulina Whitaker
Partner
Morgan Lewis

Dr. Axel Spies
Special Legal Consultant
Morgan Lewis

PeopleDoc Company Overview

500+
customers



165
countries

2.9
million users

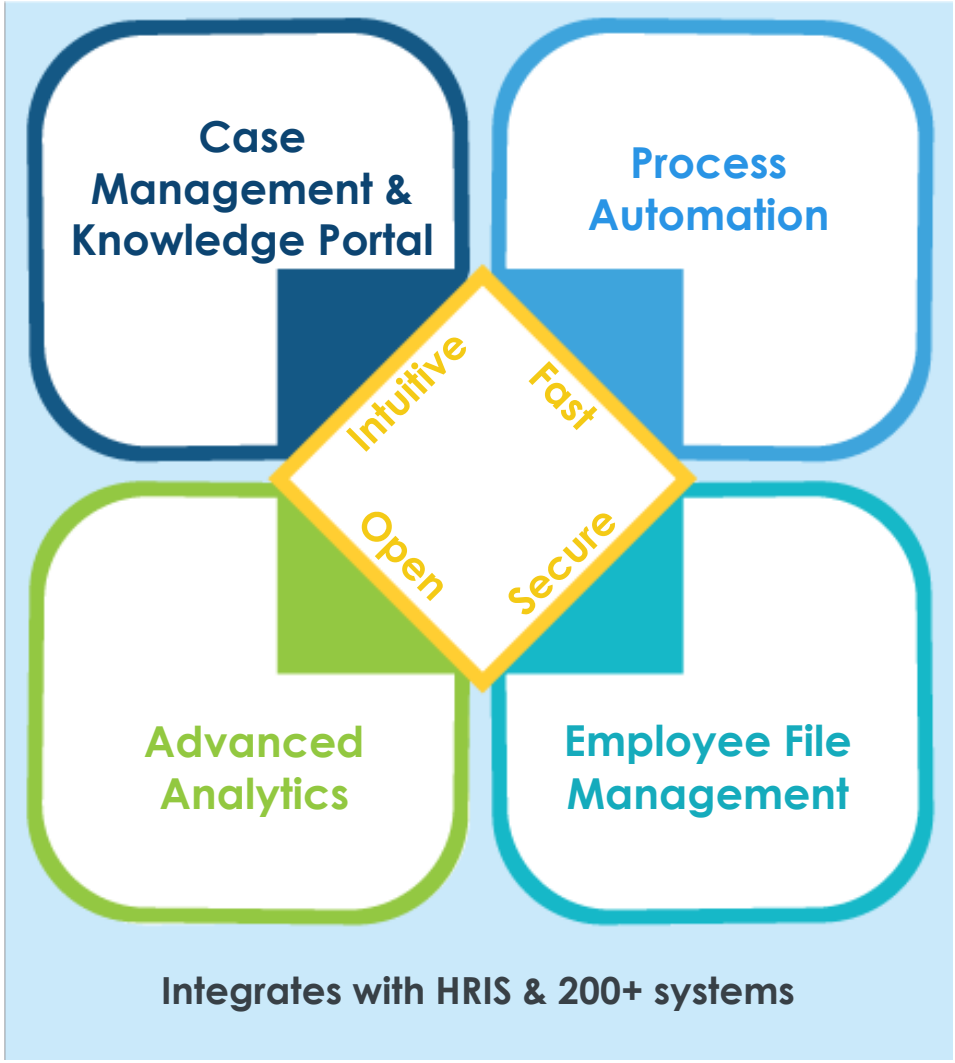
200+
systems integrated

100%
HR

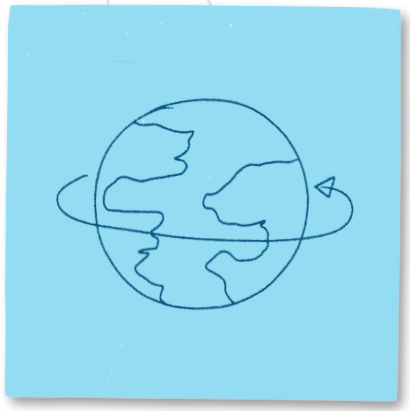
100%
customer retention

peopledoc

HR Service Delivery Platform



Why clients work with us



peopledoc

Morgan Lewis

THE GDPR: WHAT HR NEEDS TO KNOW

Pulina Whitaker
Dr. Axel Spies
Ezra Church

March 29, 2017

Overview

- Overview of the General Data Protection Regulation
- GDPR and Human Resource Issues
- GDPR and the UK
- GDPR and Germany
- Data Transfers and Privacy Shield Update
- US Perspective

SECTION 01

EU: OVERVIEW OF THE GENERAL DATA PROTECTION REGULATION

GDPR AND HR DATA

GDPR IMPACT IN UK

The New EU General Data Protection Regulation

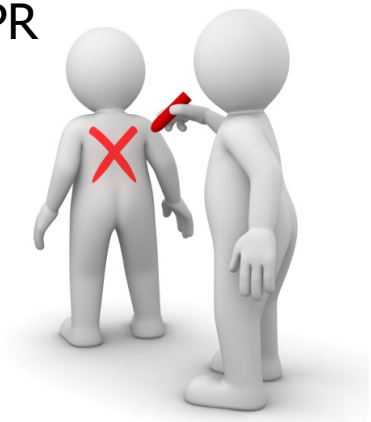
- New GDPR will replace existing EU Data Protection Directive for commercial data privacy obligations starting 25 May 2018
- "Personal Data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or 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

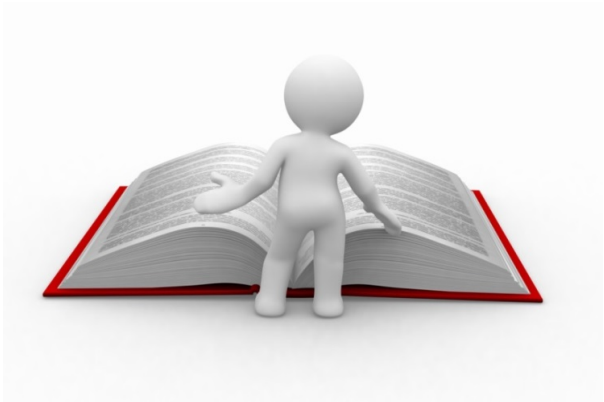
SECTION 02

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)
- 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)
  - No time for an intensive legal discussion

→ The optimistic statement that the GDPR will bring about the same standards of data protection throughout the EU is wishful thinking.

SECTION 03

US PERSPECTIVE ON GDPR

US Compliance with GDPR

- Broad application requires substantial attention by US-based companies
- Significant spending on compliance
- Fear driven by US data breach experience
- Fear of potential regulatory fines
- Unique standards not reflected in US privacy law
- Companies struggling to understand requirements and revamp their data protection mechanisms and processes to meet the requirements

US Perspective: Five Things for HR to Do

1. Identify a permissible purpose
   - In US, employee data can be collected, used and disclosed for almost any reason
   - Opposite rule applies under the GDPR—must have a permissible purpose.
   - For example:
     - Contractual necessity (e.g., for the processing of employee payment data)
     - Legal obligation (e.g., for the processing of employee data in relation to social security)
     - Legitimate interest of the employer (e.g., in the context of employee monitoring)

US: Five Things for HR to Do, cont'd

2. Be careful about relying on consent
   - In US, where employers want to collect, use, or disclose employee information in a way that is unexpected can always get consent
   - Under GDPR, processing personal data is permitted with consent of the employee, but …
     - Must be "freely given, specific, informed, and unambiguous"
     - Must be "opt-in" consent
     - Consent language must be "clearly distinguishable" from other text
   - Employees have the right to withdraw consent at any time, and must be advised of that right

US: Five Things for HR to Do , cont'd

3. Disclose and allow for employee rights
   - Access, correction, erasure, objection, and portability
   - Right to erasure—"right to be forgotten"—is new and a foreign concept in both EU and certainly under US privacy law
   - Challenge with all of these rights is the way data may be distributed throughout the enterprise.

US: Five Things for HR to Do, cont'd

4. Provide EU-based employees with robust privacy notices
   - A notice of data processing must be distributed when personal data is first collected—both for job applicants and new hires.
   - Must include many details set out in the regulation
5. Meet the new breach notification requirement
   - Most states in US have had a notification requirement for several years.
   - Notice to DPAs within 72 hours and affected employees "without undue delay."

Biography

Ezra Church
Philadelphia
T +1.215.963.5710
E ezra.church@morganlewis.com

Ezra focuses his practice on class action lawsuits and complex commercial and product-related litigation. He also focuses on privacy and data security matters, and regularly advises and represents clients in connection with these issues, including representation of companies faced with class actions, government investigations, and he has advised hundreds of companies in connection with data breaches and privacy and cybersecurity compliance issues such as data transfer, privacy policies and notice, information security policies, and online and mobile data collection. He has earned designation as a Certified Information Privacy Professional (CIPP) with the International Association of Privacy Professionals.

Biography

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.

Pulina Whitaker

London

T +44.20.3201.5550

E pulina.whitaker@morganlewis.com

Biography

Dr. Axel Spies
Washington, D.C.
T +1.202.373.6111
E axel.spies@morganlewis.com

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.

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
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

THANK YOU

Q&A

peopledoc

Thank you!

www.people-doc.com contact@people-doc.com