

**Morgan Lewis**

# **BE PREPARED FOR THE NEW EU DATA REGULATION**

**TECHNOLOGY MAY-RATHON**

Pulina Whitaker  
Dr. Axel Spies  
Charles Dauthier

May 12, 2016

© 2016 Morgan, Lewis & Bockius LLP



**SECTION 01**

# **EU-US DATA TRANSFER**

# EU-US Data Transfers

- Commission announced new “EU-US Privacy Shield” for US organizations, replacing the Safe Harbor program
  - Limitations imposed on US authorities accessing personal data for national security purposes and an oversight mechanism
  - Annual review of these principles
  - EU citizens to have the same rights of enforcement as US citizens under proposed new Judicial Redress Act
  - EU citizens and EU DPAs can complain to FTC and DoC
- Article 29 Working Party announced the Privacy Shield was not yet adequate
  - next steps?
- Three current alternatives
  1. Derogations e.g. consent to transfer outside the EU or “necessary” transfers to comply with contractual obligations or litigation management
  2. Standard Contractual Clauses
  3. Binding Corporate Rules for intra-group transfers

**SECTION 02**

**EU GENERAL DATA  
PROTECTION  
REGULATION (GDPR)**

# The New EU General Data Protection Regulation

- New Regulation will replace existing EU Data Protection Directive for commercial data privacy obligations
- “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)
- 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 new Regulation – up to higher of 4% global turnover or €20,000,000
- Individual rights to sue controllers and processors

# The New EU General Data Protection Regulation, cont'd

- Expanded application of the New Regulation's provisions
- The New Regulation 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 New Regulation 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

To do: Companies not established in the EU but processing data of EU data subjects should contemplate adopting a compliance policy

**SECTION 03**

**UK**

# UK

- The European Commissioner has said that UK-based organisations may find it harder than other European organisations to comply
- ICO agrees there are significant enhancements required under GDPR
- ICO's guidance "12 Steps to Take Now":
  1. Awareness – of key decision-makers
  2. Information you hold – audit?
  3. Communicating privacy information
  4. Individuals' rights
  5. Subject access requests
  6. Legal basis for processing personal data
  7. Consent
  8. Children
  9. Data breaches
  10. Privacy Impact Assessments
  11. Data Protection Officers
  12. International – which supervisory authority?



## UK (cont'd)

- New ICO from summer 2016 – Elizabeth Denham
- ICO guidance on PIAs
- UK Data Science Ethical Framework – for data science, Big Data or data analytics
- ICO guidance on direct marketing – recent regulatory fines
- ICO Privacy Seals – new proposal for organisations to become certified with approved operators

**SECTION 04**

# **FRANCE**

# France

- Unlike ICO, the CNIL has not yet provided guidance
- The New Regulation is not addressing some topics which are crucial to companies in France, in particular:
  - processing of personal data at the work place – legal uncertainty
  - processing of data in case of cross-border litigation – The French blocking statute “*prohibits, except in presence of treaties or international agreements and other statutes in place, the fact for anyone to request, research or communicate, in writing, orally or otherwise, documents or information of economic, industrial, financial or technical nature which are aimed at the constitution of evidence for current or future administrative or judicial proceedings outside France*”.

# France (cont'd)

## Record of processing activities:

- Revolution for French companies without a data protection officer (CIL) : towards less registration with the CNIL prior to implementing a processing of personal data
- Obligation for controllers / processors to maintain a record of all of their processing operations
- Exemption for companies employing less than 250 employees

**SECTION 06**

# **GERMANY**

# Germany

- Federal Data Protection Office has released a detailed (German) brochure on the GDPR.
- Government confident that German Data Protection Act is already in compliance, but...
- Companies are expected to do their compliance “homework” asap.
- Coordination between the State DPAs re the GDPR will be difficult (some more proactive than others)
- Focus in the near future presumably on “informed consent” and “privacy-by-design” issues as most larger German companies already have DPOs.
- Expect ‘privacy’ to become more significant in cartel proceedings.

**SECTION 05**

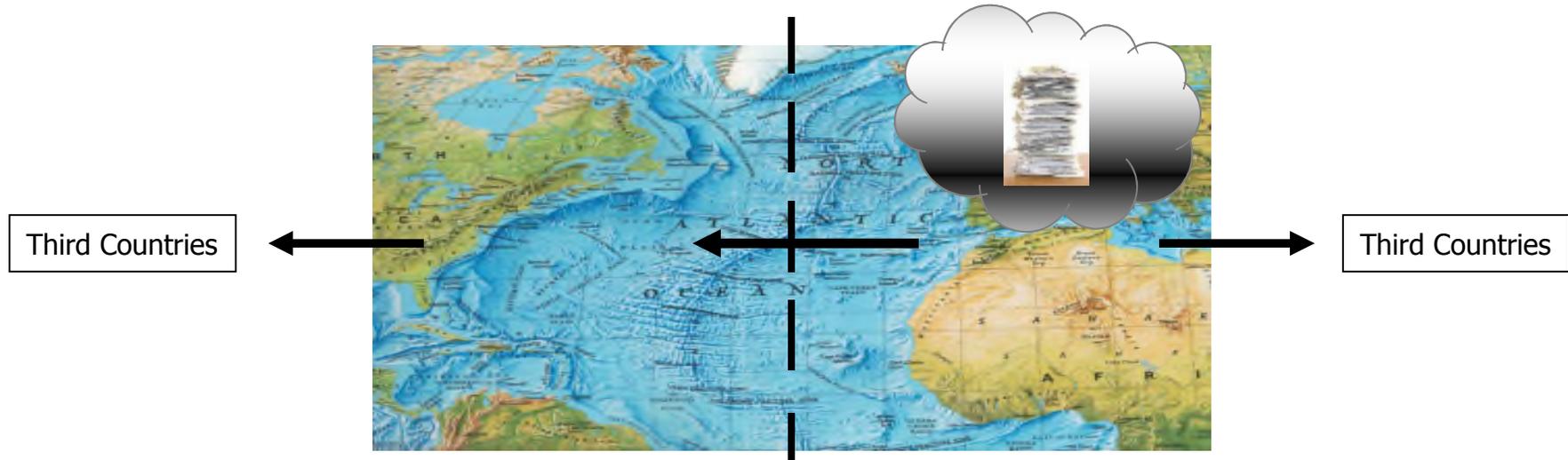
**EU-US DATA TRANSFERS  
FOR E-DISCOVERY AND US  
INVESTIGATIONS UNDER  
THE NEW GDPR**

# E-Discovery: Current Situation (Data Flows)

- Pursuant to the EU's 1995 **Data Protection Directive** (EC/46/95) and various national data protection laws, the United States is a country of "inadequate data protection." → any personal data transfer out of these countries to the US require specific legal safeguards - otherwise they are illegal.
- Various countries (e.g., France, Switzerland) have "**blocking statues**" - legal investigations by US lawyers → cooperation with US lawyers, providing evidence for US proceedings etc. without prior permission may qualify as criminal acts ("Christopher X case").
- Many US courts have ruled that these laws are not a general excuse from producing documents in Europe and apply a balancing test (cf. 1987 US Supreme Court "**Aerospatiale**" decision, 107 Sup.Ct. 2542) with uncertain outcome.

→ **US parties may be caught between a rock and a hard place because US law may require the production of evidence or discovery that may be illegal or at least restricted under the EU data protection and regulations.**

# E-Discovery (cont'd)



## EU:

- USA is a country of inadequate data protection." Privacy Shield not yet in place.
- Narrow exemption in existing Art. 26 (1) (e) EU Directive (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;
- Blocking statutes (France, Switzerland): "Legal Safeguards" needed.
- "**Letter of request**" or a "**letter of rogatory**" from the US court to the national Central Authorities under the Hague Convention on Evidence? (expensive and time consuming).
- In some countries, prior permission of the local **Data Protection Authorities** may be required.
- Special rules for **telecoms (traffic) data** and where to store them.

## Data Transfers to Third Countries:

- EU restrictions on onward transfers or use for other purposes

**Morgan Lewis**

# EU-US Data Transfers for US Discovery Purposes

## Important New Provisions in the GDPR:

- **Article 48:** Transfers or disclosures not authorized by Union Law
- *“Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.”*
- **Article 49:** Derogations for specific situations
- *“1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: [...]*
- *(e) the transfer is necessary for the establishment, exercise or defence of legal claims;”*

# Practical Consequences of the New GDPR Provisions for E-Discovery

- Scope of the new Art. 48 vis-à-vis other provisions in the GDPR
- EU/US MLATS and Hague Convention the Taking of Evidence Abroad in Civil or Commercial Matters of 1970
- EU/US Umbrella Agreement
- Judicial Redress Act of February 2016
- Impact of US appeals case, *Microsoft v. FBI*
- EU Privacy Shield for E-Discovery?
- Practical considerations (filtering data, consent requirements, data access from the US)

**SECTION 04**

# **SPEAKERS**

# 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](mailto:pulina.whitaker@morganlewis.com)

# Biography



## **Dr. Axel Spies**

Washington, DC

T +1.202.373.6145

E [axel.spies@morganlewis.com](mailto:axel.spies@morganlewis.com)

Dr. Axel Spies advises domestic and international clients on various international issues, including licensing, competition, corporate issues, and new technologies such as cloud computing in the European markets. He counsels on international data protection, international data transfers, privacy, technology licensing, e-discovery, and equity purchases. A member of the Sedona Conference on Electronic Discovery with a focus on German and international data protection, Axel is frequently quoted in the media for his telecommunications and privacy knowledge.

In addition to his telecommunications and international litigation work, Axel provides assistance to companies and industry associations on matters before US federal agencies and to investors on European mergers. He serves as the Washington correspondent and co-editor of the European telecoms journal *MultiMedia und Recht (MMR)* and the *German Journal of Data Protection (ZD)*.

# Biography



**Charles Dauthier**

Paris

T +33.1.53.30.44.74

E [charles.dauthier@morganlewis.com](mailto:charles.dauthier@morganlewis.com)

Charles Dauthier advises clients on executive terminations, collective terminations and other employment matters that surface in mergers and acquisitions, restructuring and outsourcing, and other types of reorganization. He counsels clients on employment matters attendant in employee benefits and employee representation matters. Prior to joining Morgan Lewis, Charles was an associate at another international law firm. His native language is French and he is fluent in English.

## Our Global Reach

Africa  
Asia Pacific  
Europe  
Latin America  
Middle East  
North America

## Our Locations

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



**Morgan Lewis**

# THANK YOU

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Links provided from outside sources are subject to expiration or change. Attorney Advertising.

© 2016 Morgan, Lewis & Bockius LLP

**Morgan Lewis**