

Data Privacy Developments in the EU: *Safe Harbor, Privacy Shield and the GDPR*



*Mark Partin
Managing Counsel
Oracle Privacy & Security Legal
May 10, 2016*

Agenda



- Introduction and Background on EU and US legal regimes
- Update on International Data Transfer schemes
 - What Happened to Safe Harbor?
 - EU/US Privacy Shield
- An overview of the new GDPR
 - Introduction
 - Major changes from the Directive
 - Practical considerations

How did we get here?

- Can we just blame Snowden?
- Historic and cultural differences between how the US and EU view privacy and the treatment of “Personal Information.”
- PI: United States - *Defined by various Federal & State laws*
 - Name PLUS social security number (SSN), driver’s license number, credit card #
 - Financial & Health information
 - Online credentials
- PI: EU & Elsewhere - *Information that relates to an identified or identifiable individual*
 - Non-identifiable elements
 - IP address (US v. EU)
 - Interest-based advertising data (cookie and device IDs)

Global Privacy Legal Landscape

- **US (Federal & State): many sectoral laws**
 - No national privacy or data protection law
 - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - Gramm-Leach-Bliley Act of 1999 (GLBA)
 - State laws re: security (breach notification, SSNs, data deletion, general requirements)
- **European Union (EU): one law**
 - EU Data Protection Directive (95/46/EC) + EU Member State implementing laws
 - EU General Data Protection Regulation (GDPR): one law for all of EU
 - Over 100 countries have modeled their privacy laws after the Directive

EU/US Safe Harbor

- **Problem:** EU views US privacy and data protection framework as providing inadequate protection to EU Citizens
- **Solution:** Given global need for secure trans-Atlantic data flows, the EU Commission and U.S. Dept. of Commerce agreed on the EU/US Safe Harbor program in July 2000
 - Voluntary framework based on EU Directive principles
 - Allowed for the legal transfer of EU personal information to the United States
 - Over 4400 companies were Safe Harbor certified

EU/US Safe Harbor - RIP

- Privacy activists in the EU disfavored Safe Harbor
- Snowden leaks shed light on US NSA's data collection and monitoring practices
- Austrian law student named Max Schrems sues Facebook in Ireland in 2014
- *Schrems* case reaches the Court of Justice of EU ("CJEU")
- October 6, 2015: CJEU not only sides with Schrems, but also invalidates the entire EU/US Safe Harbor Framework

Goodbye Safe Harbor - Implications

- **Invalidated #1 legal basis for transferring personal data from EU to U.S.**
 - EU citizen's right to privacy and judicial protection are undermined by US mass surveillance and storage of personal data
 - Lack of legal remedies in the U.S. for individuals who want to access, correct, or delete their data
- **Local DPAs not bound by European Commission adequacy findings**
 - DPAs can independently determine whether cross-border data transfer mechanisms comply with EU requirements, regardless of a finding by the European Commission
- **No transition period from the CJEU**
 - Oct. 15, 2015: A29WP indicated invalidation of the Safe Harbor Program was effective immediately
 - Fortunately, A29WP also indicated that the EU DPAs would not commence enforcement proceedings until the end of January 2016
- **Companies relying on Safe Harbor to transfer data from EU subsidiaries to (i) their U.S. parent company for internal operations or (ii) US-based service providers must find **alternative legal transfer mechanisms****

Alternative Transfer Mechanisms

- Model Contracts (aka Model Clauses)
 - Template contractual clauses drafted by the European Commission
 - Subprocessor flow down
- Binding Corporate Rules (BCRs)
 - Set of internal data processing and transfer rules
 - Must be approved by 28 DPAs
- Other derogations (e.g., consent of data subject)
 - Last resort, impractical
- **Safe Harbor 2.0 – Privacy Shield?**

EU-US Privacy Shield – What is it?

- Alternative to replace Safe Harbor
- Designed to re-establish the legal framework for EU/US data flows thrown into question by the invalidation of the Safe Harbor in October, 2015
- Joint effort between the US Dept. of Commerce (DOC) and the European Commission (EC)
- Final “draft” issued February 2, 2016 representing political agreement on terms between DOC and EC

EU-US Privacy Shield – Material Changes

- **Corporations**

- More transparency, more oversight
- Sanctions for non-compliance
- Notices in public privacy policy

- **Redress**

- Complaint directly against Privacy Shield participant; mandatory 45 day response
- Free ADR
- EU individuals have private cause of action in US state courts

- **US Government Access**

- “Clear limitations, safeguards, and oversight mechanisms”
- Corporations can report number of access requests
- Independent Ombudsperson to handle and investigate complaints from individuals

- **Cooperation**

- Both the FTC and FCC commit to monitor and enforce more robustly, and cooperate more with EU DPAs
- Joint, annual monitoring of Privacy Shield effectiveness, and annual report by European Commission to EU Parliament

EU-US Privacy Shield – Reaction?

- *EU Commissioner Věra Jourová*: “For the first time ever, the United States has given the EU binding assurances that the access of public authorities for national security purposes will be subject to clear limitations, safeguards, and oversight mechanisms.”
- *German Member of European Parliament Jan Philipp Albrecht*:



- A29 WP issued preliminary statement on **Feb. 3, 2016** – somewhat optimistic but concerned.
- A29 WP final evaluation published **April 13, 2016** – strong concerns; cited several shortcomings.

Privacy Shield (f/k/a Safe Harbor) - Timeline

Oct. 6, 2015
CJEU
'Schrems'
ruling

Jan. 31, 2016
End of A29WP
unofficial
grace period

Feb. 3, 2016
A29WP interim
statement
regarding the
Privacy Shield,
Model Clauses
and BCRs

Oct. 16, 2015
A29WP unofficial
grace period for
compliance with
Schrems ruling and
new Safe Harbor
agreement

Feb. 2, 2016
Political
agreement
between EC and
DoC on 'EU-US
Privacy Shield'

April 13, 2016
A29WP final
evaluation of
Privacy Shield,
Model Clauses
and BCRs

EU-US Privacy Shield – Material Issues Raised by A29 WP Final Evaluation

- **Not “Essentially Equivalent”**
 - Privacy Shield does not provide EU citizen essentially equivalent level of protection as under EU law
 - Absence of key data protection principles (purpose limitation, data retention, automated decisions)
- **Government Oversight – exceptions for national security**
 - “Massive and indiscriminant collection of personal data” not explicitly excluded
 - Ombudsperson not sufficiently independent
- **Recourse/Redress**
 - Impractical and ineffective
- **Onward transfers**
 - Need same level of protection on all aspects of Privacy Shield (including national security)
 - Should not lead to lower or circumvention of EU data protection principles

EU-US Privacy Shield – What Happens Next?

- **Article 31 Committee opinion**
 - Established under the Directive; comprised of experts representing each Member State
- EU Commission to make a final adequacy decision on whether to adopt Privacy Shield (expected in June/July 2016)
 - The somewhat negative view expressed by the A29 WP complicates matters
 - The A29 WP opinion is not binding on the EU Commission, but the A29 WP is influential and respected
 - The EU Commission will have to balance the A29 WP concerns with not wanting to delay adoption of Privacy Shield
- Even if adopted, it is a near certainty that validity of Privacy Shield will be subject to legal challenge in CJEU

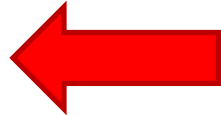
What to do now?



- Chairwoman of A29 WP confirmed that Model Contracts and BCRs can continue to serve as a legal basis of transfer
- After *Schrems*, the French and German DPAs have begun questioning data controllers about alternative transfer mechanisms upon which they are relying
- Monitor the announcements out of the EU and seek legal advice

Agenda



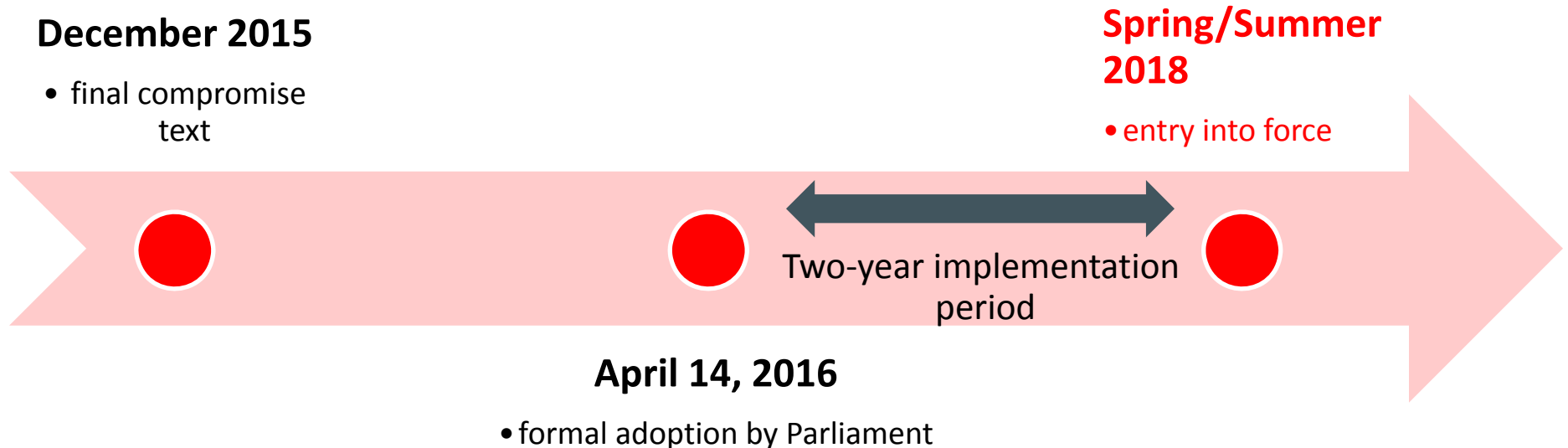
- Introduction and Background on EU and US positions
- An update on International Data Transfer schemes
 - What Happened to Safe Harbor?
 - EU/US Privacy Shield
- An overview of the new GDPR 
 - Introduction
 - Practical considerations

GDPR - Introduction

- General Data Protection Regulation (GDPR) replaces the Directive
- A single law for all 28 Member States
- No need to implement separate national legislation
- The result of four years of negotiation
- Resolves the lack of harmonization across the EU
 - But, not a complete harmonization
 - Employment law
 - Processing of health and criminal data
- Unlike Privacy Shield, the GDPR is happening
 - GDRP formally adopted by EU Parliament and already translated in the 24 official languages of the EU

GDPR – When Will It Become Effective?

- GDPR has been approved and adopted, but will not take effect until Spring 2018



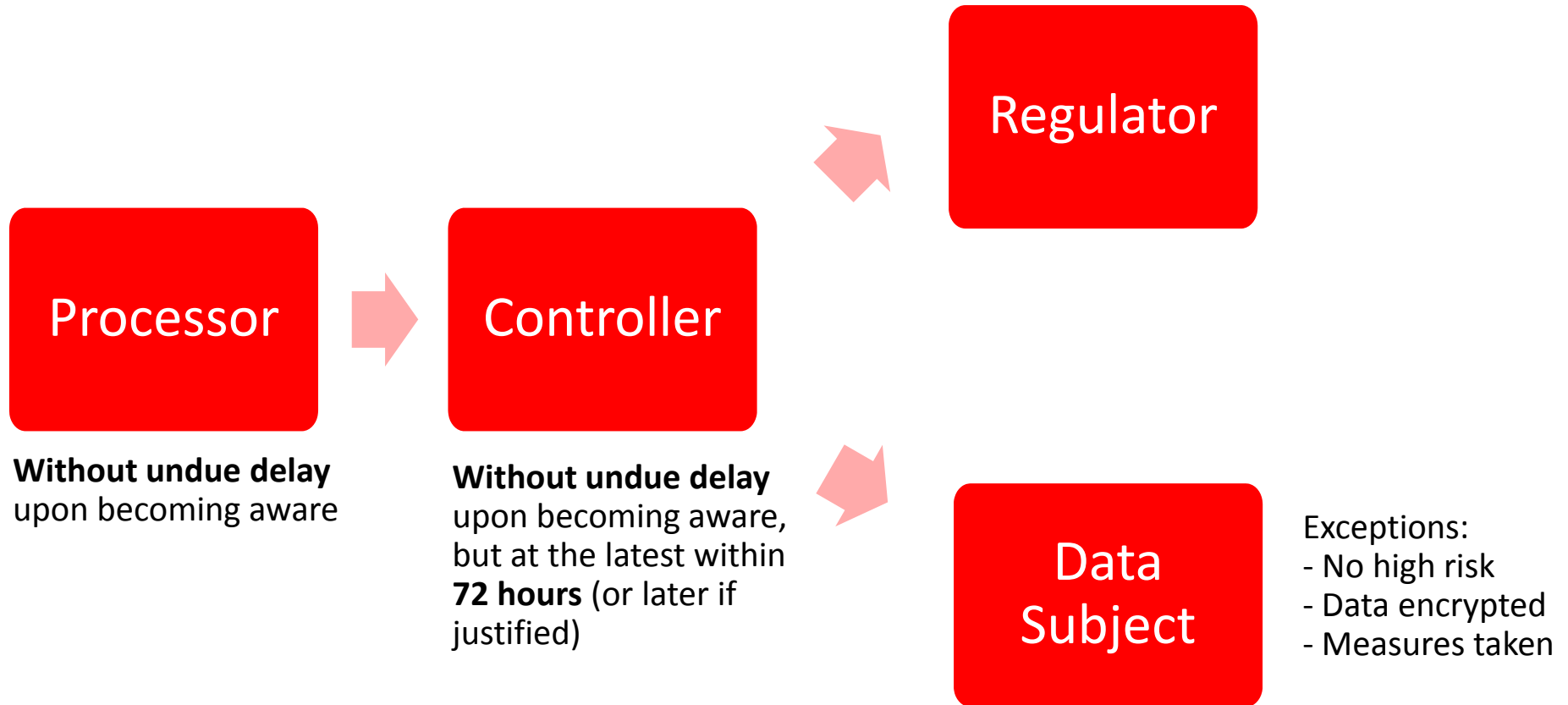
GDPR – Material Changes from the Directive

Scope expanded to include processors	<p>GDPR will apply to controllers <i>and processors</i> (i) based in the EU that process personal data, and (ii) based outside the EU who target individuals in the EU (IBA).</p> <p>Under certain circumstances, GDPR may require the processor to appoint a Data Protection Officer</p>
Records of processing activities	<p>DPA registrations are not required under GDPR; however, controllers and processors must maintain internal records of data processing activities</p>
Data protection by design and by default	<p>Controller must deploy appropriate technical and organizational controls designed to implement data protection principles and safeguards into the processing of personal data</p>
Data Protection Impact Assessments (PIA)	<p>Controllers or processors must conduct a PIA when (i) using new technologies or (ii) given the nature, scope, context and purposes of processing, if the processing poses high risk to the rights and freedoms of data subjects</p>

GDPR - Material Changes from the Directive

Definitions of “personal data” and “pseudonymisation”	<p><i>Personal Data</i> – includes location data, online identifiers, and other technology-based identifiers</p> <p><i>Pseudonymisation</i> – processing of PD such that PD can no longer be attributed to a specific data subject without additional information (which must be kept separate and cannot identifying a data subject)</p>
Enforcement and Sanctions	DPA's will have authority to investigate non-compliance and impose sanctions/fines up to EUR 20 million or 4% of annual worldwide turnover of the corporation (whichever is higher)
Consent	<ul style="list-style-type: none">• More restrictive than the Directive – implied consent no longer valid• Consent under GDPR must be freely given, specific, informed and unambiguous• Personal Data = unambiguous consent• Sensitive Data = explicit consent
One Stop Shop	<ul style="list-style-type: none">• A single national DPA as lead regulator for all EU compliance matters• DPA in the EU Member State where entity has its main presence will be responsible for decisions regarding the entity's (controller or processor) EU operations involving personal data

GDPR - Data Breach Notification



GDPR – Preparation for 2018

Raise awareness about GDPR	Ensure that management and decision makers understand GDPR is coming, and that it will require examining and potentially revising business and operational procedures and policies
Document your Personal Data	In preparation for GDPR record keeping requirements and for audit purposes, catalog the Personal Data you hold, including where it was collected and with whom it was shared
Review your privacy policies and notices	External-facing privacy policies must include certain mandatory notices, including rights of data subjects and descriptions of processing activities
Privacy impact assessments	PIAs should become part of pre-processing procedures and should be implemented as part of an overall privacy by design/default framework
Data breaches	Implement a data breach management and response plan to detect, investigate and report security incidents in accordance with the GDPR requirements and notices

GDPR – Preparation for 2018

Consents	Review your methodology for obtaining and documenting consents, especially if you have relied on implied consents or collect sensitive data
One Stop Shop	If your organization maintains a presence in multiple EU Member States, consider leveraging the “one stop shop” feature to have a single DPA across EU operations
Rights of data subjects	Examine your practices to ensure compliance with all data subject rights set forth in the GDPR, including right to object, access to Personal Data and data portability
Data Protection Officer?	Certain types of organizations are required to appoint a Data Protection Officer – determine if so required and assess where such person will sit within the management hierarchy of your organization

GDPR and Privacy Shield – Additional Points

- Until the GDPR becomes effective in 2018, the Directive remains valid and enforceable.
- Privacy Shield was designed to be future-proof – DOC and EC accounted for GDPR negotiations/drafts
- If your organization has take privacy/data protection seriously over past 10 years, GDPR compliance should not be too onerous – but, 2 years will go by faster than you think!

Safe Harbor, Privacy Shield and GDPR

QUESTIONS ?

