Managing Data Privacy in a Global Company

June 24, 2014

Bruce J. Heiman  
+1.202.661.3935  
bruce.heiman@klgates.com

Ignasi Guardans  
+32.(0)2.336.1949  
ignasi.guardans@klgates.com

Etienne Drouard  
+33(0)1.58.44.15.12  
etienne.drouard@klgates.com

Dr. Friederike Gräfin von Brühl  
+49.(0)30.220.029-415  
friederike.bruehl@klgates.com

Andrew W. Gilchrist  
+44.(0).20.7360.8148  
andrew.gilchrist@klgates.com
## MANAGING DATA PRIVACY IN A GLOBAL COMPANY

<table>
<thead>
<tr>
<th>Name</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignasi Guardans Brussels</td>
<td>EU legislative agenda and main topics of the draft EU privacy reform</td>
</tr>
<tr>
<td>Etienne Drouard Paris</td>
<td>A proven roadmap of key points to perform a cost-effective global privacy compliance program</td>
</tr>
<tr>
<td>Friederike Gräfin von Brühl Berlin</td>
<td>The future of data privacy officers and cross-border data flows</td>
</tr>
<tr>
<td>Andrew Gilchrist London</td>
<td>Consent: a core data protection right and a cultural gap within the EU</td>
</tr>
<tr>
<td>Bruce Heiman Washington D.C.</td>
<td>Alternative EU privacy regulation compliance possibilities</td>
</tr>
</tbody>
</table>
Questions for presenters

Bruce J. Heiman
Partner, Washington D.C.
Policy and Regulatory Practice Area Leader

Ignasi Guardans
Partner, Brussels
Policy and Regulatory

Etienne Drouard
Partner, Paris
Privacy, Data Protection, and Information Management

Dr. Friederike Gräfin von Brühl
Senior Associate, Berlin
Privacy, Data Protection and Information Management

Andrew Gilchrist
Senior Associate, London
Privacy, Data Protection, and Information Management
Why and how is the EU legislating on privacy?
A short guide to the Data Privacy Reform
THE BILL

Proposal

- by the EU Commission (i.e. the Government of the EU)
- A general reform “package” on data protection:
  - a General Data Protection Regulation
  - a “law enforcement” Directive

Adoption

- by the EU Parliament (i.e. direct representatives of EU citizens), acting as a sort of 1st Chamber
- by the Council of Ministers (in this case, Ministers of Justice and Home Affairs), acting as a sort of Second Chamber
CONTENT OF THE NEW REGULATION

Protection of individuals with regard to the processing of personal data

Free movement of personal data

Protection of the fundamental rights and freedoms of natural persons

Other: mandatory data protection officer; transfer of personal data to third countries or international organisations; role of independent supervisory authorities; co-operation and consistency; remedies, liability and sanctions
THE PLAYERS

Ms Viviane REDING - Directorate General for Justice (EU Commission)
(DG Connect)

European Parliament
- strong impact of Snowden’s Affair; recent elections; very high sensitivity to data protection and privacy
- several Committees involved, led by LIBE (Civil Liberties)

Governments
- High implication of Ministries competent for telcos and their experts. Detailed discussions going on at experts’ level
THE PROCEDURE FOR THE APPROVAL OF THE REGULATION

- 25 January 2012: Legislative proposal published
- 21 October 2013: Vote in Parliam. Committee
- 12 March 2014: Decision by Parliament
- Autumn 2014 (?): (Possible) adoption of the text by the Council
- 6 June 2014: Partial general approach of the Council (no trilogues)
- 2016 (?) (Possible) entry into force
A proven roadmap of key points to perform a cost-effective global privacy compliance program
SOME FEARS…
KEY POINTS OF A GLOBAL PRIVACY COMPLIANCE PROGRAM

1. Identify ‘data subjects’ and ‘purposes’
   - Customers and users (BtoB, BtoC, CtoC)
     - Sales, CRM, marketing, advertising, payment and fraud prevention
   - Employees, consultants, service providers
     - Recruitment, HR management, payroll, IT security, ethics

2. Identify data owners and simplify the map
   - Who owns the data? Who decides?
     - Identify ‘controllers’ and ‘processors’
     - Distinguish retail points of relation and online services
     - Identify the applicable laws and rely on international regulations
KEY POINTS OF A GLOBAL PRIVACY COMPLIANCE PROGRAM

3. Think global, act regional and local
   - Privacy laws reflect history and culture
     - Business models are not sufficient to design privacy policies
   - Local regulators deal with globalization at regional level
     - Feed your local counsels with your regional and global strategies

4. Privacy laws vs. other regulations
   - Coordinate Legal/Finance/Sales/Marketing/HR/IT/Ethics
   - Assess the impact of your privacy map on tax, consumer, competition and labor regulations
HOW TO PRIORITIZE VARIOUS TOPICS OF A DUE DILIGENCE PROCESS?

1. Start from the IT and legal structures
   - Time savings and reliable backgrounds
   - Localization issues
   - Identify service providers and upcoming projects

2. Ask operations
   - Sales, CRM, marketing, payment and fraud prevention
   - Recruitment, HR management, payroll, IT security, ethics

3. Come back to the board before any choice
   - Privacy issues, a crossroads of contradictory challenges
   - Obtain support before implementing any global policy
SOME TRICKY QUESTIONS…

- Compliance vs. profitability
- ‘Big Data’ and data security vs. service providers
- Cloud computing vs. data transfers
- Data retention vs. business value and discovery
- CONSENT vs. consent
- Ongoing draft regulations
WHERE IS THE VALUE?*

1. **A centralized diagnosis** *(2-4 months)*
   - 15% of the cost, a critical starting point

2. **Local compliance assessment** *(3-6 months)*
   - 50% of the cost, a necessary step

3. **Global compliance implementation** *(2-6 months)*
   - 20% of the cost, the final outcome

4. **Global compliance recognition**
   - 15% of the cost

*Example for a compliance program in +/- 40 jurisdictions*
The future of data privacy officers and cross-border data flows
DATA TRANSFERS WITHIN THE EU

Current legal status

Data transfers within the EU:
- **General rule:** Collection of personal data within a member state triggers the national law of that member state.
- **Exception:** If data processing is carried out by an entity located outside the member state but within the EU, the national law of the business entity’s location is applicable.
- **Consequence:** Data processing in Europe is carried out in member states with the lowest data protection standards.

Expected impact of EU Regulation

- Regulation is directly applicable
- Harmonization of data protection standards in the EU
DATA TRANSFERS BETWEEN EU AND NON-EU COUNTRIES

Current legal status:
Adequate level of data protection necessary
- Formally determined by the EU Commission
- Binding corporate rules + authorization
- Individual agreement + authorization
- EU Standard Clauses
- Safe Harbor Agreement
- Consent

Expected EU Regulation:
- Commission may make positive and negative decisions
- Harmonized criteria for binding corporate rules
- Individual agreement authorized by supervisory authority needs European Commission’s approval
- Individual case-by-case authorization by supervisory authority
WHAT IS A DATA PROTECTION OFFICER (DPO)?

- **Characteristics**
  - Independent individual who has been appointed by a private or public body to ensure data protection compliance
  - Special qualification, time and resources to fulfill obligations as DPO

- **Tasks and obligations**
  - Working toward compliance with data protection law
  - Cooperation with data protection authorities
  - Contact person for employees and any other data subjects

- **Strong and independent position**
  - Not bound by any instructions
  - Controller/processor is obliged to support the DPO
  - Indefinite or fixed-term appointment
  - Strong protection against being dismissed
WHAT CAN WE EXPECT ON THE EU LEVEL?

- **Mandatory appointment of DPO**
  - Private/public body employs 250 people or more
  - Core activities of private body require processing operations with regular and systematic monitoring

- **Differences to the German model**
  - Similar role of DPO as to qualification, position and tasks
  - A group of companies may appoint one single DPO
  - Different threshold for mandatory appointment of DPO
  - Minimum appointment for at least 2 years
Consent: a core data protection right and a cultural gap within the EU. Consent requirements for cookies and in the draft data protection reform
CONSENT AS A CENTRAL CONCEPT

- Article 2 (h) of Directive 95/46/EC: “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”.

- What does this mean? Working Party – acknowledges scope is wide but must be unambiguous. Passive behaviour enough? Where on scale do you imply consent?

- Not all activities require consent: Article 7 (f) – “where necessary for the purposes of the legitimate interests pursued by the controller”.

- Member states tasked with implementing directive into its own national laws. Sometimes they get it wrong!

- Nov 2011 – two Spanish trade associations successfully challenged Spanish legislation as being contrary to EU law: it wrongly transposed Article 7(f) by adding in a further restriction that information must be available in public databases.

- Decision highlighted that lack of harmonisation causes trouble for multinational companies!
REQUIREMENTS ON “COOKIES”

 “A cookie is a small file, typically of letters and numbers, downloaded on to a device when the user accesses certain websites. Cookies allow a website to recognise a user’s device.”

 Directive 2002/58/EC (“e-privacy Directive”) of 12 July 2002: have to provide clear and comprehensive information about cookies, and an “opt out”.

 Changes introduced by Directive 2009/136/EC (the so-called “Cookies Directive”) : introduced a consent requirement. To be understood by reference to the DPD.

 This legislation is complementary to, and does not supersede, Directive 95/46/EC (“DPD”).
EUROPEAN DIVERGENCE

- Transposition into national laws was required by 25 May 2011 (In the UK – through Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (Regulations) which amended 2003 Regulations.

<table>
<thead>
<tr>
<th>Article 29 Working Party</th>
<th>UK ICO</th>
</tr>
</thead>
<tbody>
<tr>
<td>must be clear to users what action signifies consent – positive action / behaviour – tick a box</td>
<td>Generally speaking implied consent inferred from cumulative actions enough</td>
</tr>
<tr>
<td>Prior consent necessary before cookie is placed.</td>
<td>Recognises commercial reality – “where possible”</td>
</tr>
<tr>
<td>no distinction between types of cookies – though recognises proportionality</td>
<td>Recognises higher standard for “intrusive” cookies</td>
</tr>
<tr>
<td>Has led to some more stringent approaches – for example Belgium and Poland.</td>
<td>ICO has said it will take proportionate action, but not likely to be high on agenda.</td>
</tr>
</tbody>
</table>

- As of 6 May 2013, cookie consent requirements had been adopted in 24 out of 30 EEA Member States. For example, Germany has not yet implemented.

- Different enforcement powers? For example, first fines in Spain - 3,500 EUR. UK Regulator more relaxed? Jan – Mar 2014 – 65 complaints (cookies) / 34,530 complaints (SPAM). Under 1,000 total since April 2012. Notification requirements?

- Most websites international – businesses forced to adopt highest common denominator?
APPLICABILITY FOR WEBSITE OPERATORS OUTSIDE EUROPE?

- Can you escape the rules if your website is hosted and operated by a company overseas?

- Is it targeting a European country? Are you placing cookies on the website user’s computer?

- Do you have an office, branch or agency in that country? If not, enforcement power may be limited.

- If you operate as part of a Group, you can’t necessarily rely on fact that your European subsidiaries aren’t technically the one’s processing the data / operating the website following Google Spain – CJEU – May 13 2014
PROPOSED DATA PROTECTION REGULATION

- Adds in the words “explicit”. Requires statement / positive action – i.e. tick box.

- Little room for misinterpretation, but too rigid? In the UK, we often rely on implied consent – so major change in practice

- Will it conflict with E-Privacy Directive? Will it supersede it?

- Draft regulation may not complete its passage until 2015 – and would likely not come into force for a further 2 years.
Alternative EU privacy regulation compliance possibilities
US-EU SAFE HARBOR

• History

• Substance
  ▪ Transparency
  ▪ Seven Principles
  ▪ Enforcement

• EU Re-examination
  ▪ Data Flows↑
  ▪ Number of Safe Harbor Companies↑
  ▪ And Then the Snowden Disclosures!
US-EU SAFE HARBOR (con’t)

• EU Reaction to Snowden Disclosures Highly Critical
• Commission Report November 2013
  With 13 Recommendations to:
  ▪ Enhance Transparency
  ▪ Improve Redress
  ▪ Tighten Enforcement
  ▪ Limit USG Access
• USG Response on Snowden
  ▪ President Obama Speech, PPD 28
  ▪ FTC Enforcement
  ▪ Administration Decision to Change/End Bulk Collection
  ▪ Attempt to Reach Bilateral Intelligence Agreement with Germany
• Two Remaining Issues
  ▪ #3: Sub-Contractor Obligations
  ▪ #13: National Security Exception
• Prognosis and Timing
TRANSATLANTIC TRADE & INVESTMENT PARTNERSHIP (TTIP)

The Basics
- Rationale
- Agenda

US Data Objectives
- Enable cross border data flows
- Prohibit localization requirements

EU Silent?
- Nothing Specific in TTIP
- Hint in WTO Financial Services Talks?

Timing and Prognosis
EU DATA PRIVACY REGULATION

Protection From New Requirements

IF  US – EU Safe Harbor

THEN  TTIP
QUESTIONS?

Bruce J. Heiman
Partner, Washington D.C.
Policy and Regulatory Practice Area Leader

Ignasi Guardans
Partner, Brussels
Policy and Regulatory

Etienne Drouard
Partner, Paris
Privacy, Data Protection, and Information Management

Dr. Friederike Gräfin von Brühl
Senior Associate, Berlin
Privacy, Data Protection and Information Management

Andrew Gilchrist
Senior Associate, London
Privacy, Data Protection, and Information Management