EU General Data Protection Regulation

“Databeskyttelsesdagen 2015”

Copenhagen

John Bowman, Senior Principal
Promontory Financial Group, London

jmbowman@promontory.com

+44(0) 20 7997 3417

28 January 2015
Ordinary legislative procedure (co-decision)

January 2012
- INITIAL CONSULTATION
- INSTITUTIONAL FEEDBACK

Q2/3 2015?
- TRILOGUE
- TEXT AGREED

Q4 2015?
- COMPROMISE TEXT

Q1 2016?
- IF EP AND COUNCIL VOTES PASS; REGULATION IS ADOPTED
- IF EITHER EP AND COUNCIL REJECTS DRAFT; FURTHER NEGOTIATIONS

Q1 2018?
- REGULATION GOES LIVE
The state of play

“You should also oversee, during the first six months of the mandate, the conclusion of negotiations on the reform of Europe’s data protection rules as well as the review of the Safe Harbour arrangement with the U.S.”

Jean-Claude Juncker, President-elect of the European Commission, mission letter to Andrus Ansip, Vice-President for the Digital Single Market, 10 September 2014

“We made it! #EUdataP”

Jan Philipp Albrecht, European Parliament Rapporteur for General Data Protection Regulation, on Twitter after LIBE Committee voted to adopt a compromise text, 21 October 2013

Nothing is agreed... until everything is agreed

Council of the EU DAPIX Working Group in Brussels

...but partial general approach obtained on third country transfers, risk-based approach, and public sector exemptions under Greek and Italian Council Presidencies. Latvian presidency H1 2015.
Some key issues and impacts
Expanded scope

**Material and Territorial scope:**
Scope of ‘personal data’ extended to include cookies and IP addresses; the GDPR applies to the processing of personal data of EU residents regardless of the location of data controller/processor;

**Impact:** Expanded scope could cut across certain businesses processes and models, e.g. online behavioural advertising and data analytics. Businesses that operate outside the EU will need to appoint a representative in the EU.

**Explicit consent:**
The only consent allowed is explicit. Burden of proof is on the data controller to demonstrate that explicit consent has been obtained;

**Impact:** Increased collection costs; reduced take-up rates and risk that data sets cannot be fully utilized. Impact on advertising sector and digital economy generally.
Enhanced rights

Right to be forgotten:
Data controllers will need to inform third parties of a data subject request to erase personal data;
Impact: Costly to implement and manage process to deal with requests. Would affect search, print, broadcast and social media in particular.

Right to data portability:
The data subject will have the right to obtain their personal data in a commonly used structured format;
Impact: Cost of updating systems. Would affect utilities, telecoms, financial services and retail.
**Additional obligations**

**Measures based on profiling:**
The data subject will have the right not to be subject to a measure based on profiling where it legally or significantly affects them;

**Impact:** Direct impact on advertising and credit reference agencies. European Parliament proposals require manual decision where profiling produces legal effect or significantly affects the individual.

---

**Data protection by design and default:**
The data controller must embed data protection by design and default into systems design and processes, and must implement appropriate measures to ensure the protection of the rights of the data subject;

**Impact:** Potential costs on businesses with large and diverse systems, particularly where legacy systems need to be upgraded or replaced. Long lead-in time on IT programmes means current projects may be affected.
Additional obligations

**Data breach notifications:**
The data controller shall without delay and where feasible notify the supervisory authority of a breach within 24 hours (European Parliament and EU Council suggest 72 hours);

**Impact:** UK Government impact assessment calculates costs of new reporting requirements at £30-£130 million for UK business per annum.

**Data protection impact assessments:**
Data Protection Impact Assessments to be carried out where the data processing presents specific risks; projects in scope are likely to be wide;

**Impact:** UK Government impact assessment calculates cost at £70-£80 million for UK business per annum. Data controllers will need to focus on handling of sensitive data and build in carrying out data protection impact assessments early into the project management design process.
Additional obligations

**Data Protection Officers:**
To be mandatory except for small and medium enterprises with <250 employees where processing ancillary to core activities;

**Impact:** UK impact assessment calculated cost at £35-£75 million for UK business per annum. EU Council prefer non-mandatory risk-based appointments. European Parliament wants DPOs to be appointed where >5000 subjects data processed per annum.

**Data transfers to outside the EU:**
Adequacy decisions, model clauses, contracts and binding corporate rules are all permitted;

**Impact:** All binding corporate rules and non-standard contracts will require pre-approval of supervisory authorities; costly and time-consuming. “Anti-FISA clause” in European Parliament text could create conflict of law issues arising. EU/US Safe Harbour still under review by Commission and ECJ case pending.
Stronger and more consistent enforcement

**One-Stop Shop:**
The competent supervisory authority will be where the “main Establishment” of the data controller is located;

**Impact:** Significant for multi-national businesses which would prefer to have a single ‘home’ supervisory authority. Issue of local access by data subjects still to be resolved

---

**Sanctions:**
Maximum fines of €1million or 2% global turnover, whichever is higher. Member States may lay down rules on penalties;

**Impact:** High fines may lead to risk-averse approach and therefore higher costs. European Parliament is proposing fines of €100 million or 5% global turnover, whichever is higher.
Will we get consistency?

**YES**

- A **Regulation** has to be applied directly: theoretical consistency in most areas;
- The **European Data Protection Board** will own the consistency mechanism and may have own agenda;
- The **European Court of Justice** will continue to make pan-European rulings; and
- The **Commission** can adopt **delegated and implementing acts** but uncertainty on scope and timing.

**NO**

- Some **opt-outs and member state flexibility in Regulation** (e.g. freedom of expression, public sector, employment, research);
- **Local Data Protection Authorities** will still interpret the Regulation in their guidance and enforcement actions; and
- **Cultural and social norms** will still differ, affecting press coverage, consumer reaction etc.