Data Protection Legal Issues
BCS / EEMA Future Privacy and Identity
10 December 2015

Kuan Hon
Consultant Lawyer

kuan.hon@pinsentmasons.com
Introduction

- Self – 4 x 2 x
Outline

- Data protection laws – current position
- Proposed General Data Protection Regulation (GDPR)
- Issues / problems
DATA PROTECTION
Data protection (DP)

- Data Protection Directive 1995 – main focus here
  - Based on Council of Europe’s Convention 108
- DP also under EU Charter of Fundamental Rights
  - ( != Council of Europe’s Convention of Human Rights )
  - DP right, separate from privacy right
- Cf. laws / rights re. e-Privacy Directive, misuse of private information, confidential information, etc. etc.
1995 Data Protection Directive

- Objective – dual purpose
  - Free flow within EEA + high minimum DP standards
- Directive - implemented by national laws; *not* harmonised
  - Cf. Regulation

- Regulates “processing” of “personal data” of “data subjects”
- Supervised by data protection authorities ( DPAs ) – UK ICO
Data protection basics

• “Data subjects” - live humans only (national differences)
  – non-EEA individual too – human rights
• “Personal data” - broad – eg aircraft engine data
• Automated “processing” – also v. broad, > IT def.
  – storage, transmission, disclosure, display / viewing, spam / malware filtering...
• Legal obligations on “controller” to comply with DP principles (non-EEA too)
  – Determines “purposes & means” (individuals, charities)
  – Incl. on use of third party “processors” eg cloud providers
    • choose processor – sufficient guarantees on “security”;
      written contract (instructions, security); ensure compliance
Data protection principles

- Collection, disclosure / sharing & use of personal data
- Principles – fair & lawful processing; purpose limitation; data minimisation; accuracy; retention / deletion; + legal basis eg consent; security; direct marketing; data subject rights eg access / correction
  - “Special category” sensitive data, eg health
  - “Transfer” of personal data outside EEA restricted too
- Data subject rights & remedies – courts, DPAs
- NB - “consent” basis ( vs. legitimate interests ); public personal data ( eg tweets ); other myths
GDPR
GDPR objectives

- Individuals - strengthen rights, increase control
- Organisations - facilitate cross-EU business / operations by providing a single set of data protection rules across all EU Member States; remove unnecessary administrative requirements

“...a more prescriptive approach will not necessarily bring about better data protection” – ICO, April 2012
January 2012 – Commission

March 2014 – European Parliament

GDPR

June 2015 – Council of Ministers

Q1 2016 ? – settled text
+ 2 years + delegated / implementing acts / EDPB
Hello,

Thank you for contacting Online Customer Support.

We are writing to you in relation to your query about a price request for the EU General Data Protection Regulation to go through either before the end of 2015, by the end of March 2016, by the end of June 2016.

We have checked with our Trading team and they have confirmed they would not be able to offer any odds for your request.

However, we would like to encourage you to take advantage of our betting opportunities currently available on site. For a variety of markets for Politics, please navigate to the following link:

Key changes

- Accountability – including **data protection by design & default**; info, **records / logs**; DPIAs ( > security ); **DPOs**; certifications, **seals, codes** etc; enhanced **DPA powers** – audit, fines
- Enhanced data subject rights – no access fee; data portability, erasure; “class actions”
- Expansion in territorial scope – but…
- Controllers / processors – NB **direct processor liability** - contracts
- “Personal data” definition, consent
- Security incl. **breach notification** to DPAs & individuals
- International transfers
- Abolition of notification / registration fees; one-stop shop
- Profiling / automated decision-taking
Largest ICO Fine v Large FS Co’s Global Turnover

- Largest ICO Fine 2010
- Largest ICO Fine 2011
- Largest ICO Fine 2012
- Largest ICO Fine 2013
- Largest ICO Fine 2014
- Largest ICO Fine 2015
- Large FS Co Annual Turnover 2014 (%)

- 5%
- 2%
- 1%
- 0.50%
- Fine
ISSUES / PROBLEMS
GDPR big picture implications

- “Regulation” doesn’t mean better harmonisation
  - Member State discretion / room for manoeuvre built-in
    - national laws can restrict data subject rights for “important objectives of general public interest”, etc
  - Ambiguities - some deliberate, in the past…
    - Newt Minow’s quote – Germany, France, Soviet Union, Italy
- Better DP for data subjects? – maybe; restrictions, public sector
- Better for controllers? – fee abolition; one-stop shop…
- For cloud computing, big data, IoT etc?
  - Services to EEA customers withdrawn - or laws ignored?
- Better for public sector processing of personal data…!
“Personal data”

- The trigger – both binary & analogue aspects
  - Location data, IP addresses, device identifiers
    - Should everything be “personal data”?  
    - If everything is “personal data”…
  - But privacy is contextual! Purpose & method etc. do matter
    - E.g. IP address
      - Count unique visitors to a site, vs. stalking someone across the Web
- Risk-based approach? Cf. security risks; DP as the new “health & safety”? “Because of data protection”
Consent

- Explicit consent under the GDPR? (vs. unambiguous)
- Conditioned to consent…?

Trained to Accept? A Field Experiment on Consent Dialogs

Rainer Böhme
International Computer Science Institute
Berkeley, California, USA
rainer.boehme@icsi.berkeley.edu

Stefan Köpsell
Technische Universität Dresden
Dresden, Saxony, Germany
stefan.koepsell@tu-dresden.de

ABSTRACT
A typical consent dialog was shown in $2 \times 2 \times 3$ experimental variations to 80,000 users of an online privacy tool. We placed emphasis on the principle of informed consent across jurisdictions [5]. Anecdotal evidence, intuition (from introspection), and empirical studies on various forms of interventions all
Nobody reads terms and conditions: it's official

Not one customer of online computer game seller Gamestation read the terms and conditions of sale on 1st April, the company has said. In an April Fools' Day prank, it has claimed the legal right to the souls of all those customers. | 19 Apr 2010
Why the idea of consent for data processing is becoming meaningless and dangerous

Data protection

Data consent Part Two: For the sake of Europe’s privacy, it’s time we moved on from the unworkable consent model

Competition, Data protection, Privacy policics, Regulatory action
Short of consent: right to object and opt-out mechanisms
Beyond consent: user control and sharing the benefits
New, innovative ways to provide information, access and control to individuals

Opinion 7/2015
Meeting the challenges of big data
A call for transparency, user control, data protection by design and accountability
Paid vs. ad-supported etc. models

- Conditional consent (Parliament)
- The right balance?
Security

• Separate law, or under data protection?
  – Security under GDPR -

• Proposed NIS Directive; sectoral?

• “Strict” liability for security?
  – GDPR – processors’ liability ( >> security )
    • Pinsent Masons video
      https://vimeopro.com/pinsentmasonspreseas/gdpr-seminars & SCL article
    – HP patches report - software vendors?

• Breach notification?

• In practice...
Competitiveness, consumer choice

- Money spent on model clauses etc., more prescriptive, broad GDPR compliance requirements
- Costs will be carried by consumers...
- Favours large incumbents over SMEs, eg cloud

- Consumer protection, competition law
Price discrimination / personalised pricing

• Example - travel sites & cookies

• Would GDPR’s profiling / automated decision-taking provisions help?
Neutral intermediaries - defences

- EU E-Commerce Directive
  - Not data protection issues!
  - GDPR unclear... legal uncertainty

- Special status for personal data >> IP?

- In practice... processors e.g. cloud
Technology-neutrality – esp. cloud

• Eg “transfer” restriction – location fixation – necessary?
  – Physical location as proxy for access & jurisdiction
    • Based on mainframes, tapes / punched cards etc
  – Link broken – availability of remote access + encryption
    • Microsoft warrant case in US
• What would you prefer –
  – stored in EEA, unencrypted on open server, or
  – stored in the US, AES 256 encrypted (keys accessible in EEA only)?
• It is what it is… practical points on Schrems & Safe Harbour
Enforcement

• Detection + enforcement
• Detection
  – Hence breach notification laws, though evidence...
• Enforcement
  – Individuals’ resources vs. large corporations
    • “Class actions”?
  – DPA resources to detect / enforce breaches
    • UK - ICO £18m from registration fees
Mass state surveillance

Digital surveillance 'worse than Orwell', says new UN privacy chief

Joseph Cannataci describes British oversight as ‘a joke’ and says a Geneva convention for the internet is needed

- GDPR anti-FISA clause... fears re “transfers”
- But – national security; UK Investigatory Powers Bill etc
- International solution needed! (+ encryption)
Ways to legislate / regulate

- 2 types of law
  - Precise rules vs general principles
- Technology-neutral view
  - collection / disclosure / sharing / use (+ condition)
  - security as *enabler* for control of access to data
- General: “Don’t Do Devilish or Dodgy Deeds with Data that Disadvantage Doeses”!
  - + specific guidance / codes

- But - prescriptive GDPR unstoppable…?
5. In the context of the European Council’s objective to conclude the reform by the end of the year, the Presidency submits for examination with a view to confirmation to the Permanent Representatives Committee compromise suggestions on the main outstanding issues relating to all the Chapters of the draft General Data Protection Regulation. On the basis of the outcome of this examination, the Presidency is engaged in trilogue with the European Parliament with the aim to find an early second reading agreement.

6. All the Chapters have been examined intensively by experts and JHA Counsellors when preparing the eight trilogues with the European Parliament that have taken place since June 2015 on all the Chapters of the General Data Protection Regulation. The Presidency sought
What we need

- Sensible, achievable, technology-neutral laws, that strike an appropriate balance with other societal interests
  - If impossible to comply, will breach...
- Practicable enforcement – DPAs (resources), individuals
  - And carrots not just sticks
- State surveillance – international agreement!

- But what will we get? Jury is out...
Thank you!

Kuan Hon

Email: kuan.hon@pinsentmasons.com