CharlesRussell Speechlys

Data protection – past, present and future

Robert Bond, CCEP, Head of Data Protection & Cyber Security Law Group

PROTECTION OF PERSONAL INFORMATION…

•… is nothing new

- Right to privacy according to Samuel Warren and Walter Brandeis
  - 1890
  - Right to be let alone
- European continental countries – right to privacy embedded in early constitutions
  - “Private life” referred in the French Constitution of 1791
  - Portuguese Constitution of 1822 set up the secrecy of letters
- Greatest recent examples of misuse of personal information
  - WW2 German occupied countries
  - 20th century European dictatorships
- **Privacy of personal information is not exclusive of the internet connected era!**

AND THEN IT GOT COMPLICATED!

- Advent of computerised world: storage / exchange of large quantities of information
  - Facilitated
  - Lost the strong connection with tangible world
- Data protection legislation developed from the early ’70s onwards
  - Land of Hesse Act (1970)
  - Swedish Data Act (1973)
  - Portuguese Constitution (1976)
- UK – Data Protection Act 1984

LEGAL FRAMEWORK

UNITED STATES	EUROPE	ASIA
About 20 sector-specific laws and hundreds of state laws	EU Data Protection Directive transposed into national law in 28 different member states	Varying national laws loosely based on the European Directive
e.g. HIPAA (The Health Insurance Portability and Accountability Act) and COPPA (Children's Online Privacy Protection Act)	e.g. The UK Data Protection Act 1998, Germany's Federal Data Protection Act 2001 and Italy's Privacy Code 2003	e.g. Malaysian Personal Data Protection Act 2010 and South Korea's Personal Information Protection Act (PIPA) 2011

REGISTRATION/NOTIFICATION REQUIREMENTS

UNITED STATES	EUROPE	ASIA
No requirement for companies to register	Requirements vary but most countries require registration before the processing of personal data	Varies according to country, and in countries such as Malaysia it is dependant on sector
No national Data Protection Authority (DPA)	Each member state has a DPA, but those DPAs have varying levels of expertise, funding and resources	DPAs are generally in their very early stages or operate at a regional level (if they exist at all)

COLLECTION AND PROCESSING

UNITED STATES	EUROPE	ASIA
Vary widely but generally require pre-collection notice and opt-out for use and disclosure of regulated personal information	Data controllers need to meet one of several conditions to collect and process personal data such as: - Consent - Legitimate reason - Performance of a contract - Protecting the data controller's vital interests	Requirements vary across the Asia-Pacific region but the fundamental principles of the European Data Protection Directive can usually be found in the various national laws e.g. purpose definition and use limitation
Opt in rules usually apply where information is considered 'sensitive' e.g. health information, children's information	There are stricter rules for processing sensitive personal data (e.g. gaining a data subject's explicit consent)	Countries such as South Korea, Singapore and Malaysia may take a strict view on how personal data is processed

TRANSFER

UNITED STATES	EUROPE	ASIA
No geographic transfer restrictions apply out of the US	Within the EEA is permitted. There are conditions to be met to transfer data out of the EEA such as: - Consent - Legitimate reason - Performance of a contract - Protecting the data controller's vital interests	Different restrictions apply but many reflect the conditions listed in the European Directive
	'Adequate protection' is required for transfers outside of the EEA e.g. "approved countries", Model Clauses and BCRs	APEC Cross Border Privacy Rules

SECURITY AND BREACH NOTIFICATIONS

UNITED STATES	EUROPE	ASIA
Most businesses are required to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information	Data controllers must take appropriate technical and organisational measures	Varying standards expected – from detailed provisions in South Korea to more general expectations in Malaysia and Singapore
HIPAA regulated entities are subject to much more extensive data security requirements	These measures are aimed to prevent unauthorised processing, accidental loss or damage to personal data	Range from mandatory notifications in South Korea to no notifications in Singapore and Malaysia
Breach notifications are commonplace across the States	No mandatory breach notifications under the Directive but different obligations across Europe are in force	

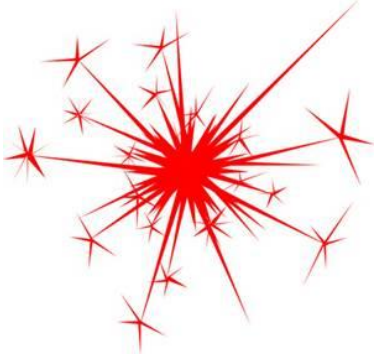
ENFORCEMENT

UNITED STATES	EUROPE	ASIA
Violations generally enforced by the FTC, State Attorney General, or the regulator for the industry sector in question	Violations enforced by each country's respective DPA. Generally range from $'000s to $'000,000s	Violations enforced by each country's respective DPA. May be up to $800,000 in Singapore
Highest penalty - $100m against LifeLock (Dec 2015)	Highest penalty - $4.5m by Portuguese DPA	DPAs in relatively early stages so not much fining history
Possibility of class action lawsuits	Google fined $1.2m by Spain	But some DPAs even provide for imprisonment for relatively minor offences!

The General Data Protection Regulation

It's finally here!!

- http://www.europarl.europa.eu/news/en/news-room/20151215IPR07597/Data-protection-package-Parliament-and-Council-now-close-to-a-deal
- http://europa.eu/rapid/press-release_IP-15-6321_en.htm
- http://www.pdpjournals.com/proposal-gdpr-final-compromise.pdf



The New General Data Protection Regulation

Scope (Articles 2&3)

- No surprises
- Applies to controllers and processors
- Has extra-territorial applicability

The New General Data Protection Regulation

Consent (Articles 4, 7, 8)

- Much debated and contested
- Any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement of by a clear affirmative action, signifies agreement to personal data relating to them being processed
- It shall be as easy to withdraw consent as to give it
- Children – at least 13 and up to 16 years – up to each member state

The New General Data Protection Regulation

Information and access to data (Articles 14, 17, 18)

- Privacy policies will need to be up-dated!
- Divided into requirements when data collected directly from individuals and **not** collected from individuals
- Right to erasure / “right to be forgotten”
- Right to data portability

The New General Data Protection Regulation

General obligations (Article 22)

- Emphasis on ‘demonstrating’ compliance
- ‘Such measures shall be reviewed and updated where necessary’
- ‘…where proportionate [this] shall include the implementation of appropriate data protection policies by the controller’
- ‘Adherence to approved **codes of conduct** pursuant to Article 38 or an **approved certification measure** pursuant to Article 39 may be used as an element to demonstrate compliance with the obligations of the controller’

The New General Data Protection Regulation

General obligations (Articles 25, 26, 28)

- Controllers or processors processing data of EU citizens but not located in the EU will have to appoint a **representative**
- **Processors** prohibited from enlisting another processor without prior specific or general consent of the controller. In the latter case will always have to inform controller of any intended changes concerning the addition or replacement or processors
- Extensive requirements for data processing contracts
- Controllers / controllers' representatives shall maintain a record of processing activities under its responsibility – the Regulation prescribes what exactly this should comprise

The New General Data Protection Regulation

Data Protection Impact Assessments and Prior Consultations (Articles 33)

- Requires where ‘using new technologies’ and where potentially high risks for individuals’ privacy rights and consult with DPA where risks are particularly high

The New General Data Protection Regulation

Data Protection Officer – Article 35 onwards

- Mandatory appointment in certain circumstances, e.g. where there is the “regular and systematic monitoring of data subjects on a large scale” or where the “core activities” mean that the controller or processor will process a large volume of “special categories of data” or “data relating to criminal convictions and offences”

The New General Data Protection Regulation

Other points of interest…

- One stop shop
- Right to compensation for data subjects for material or immaterial damage
- Max fines – EUR 20million / 4% total worldwide annual turnover of preceding financial year, whichever is the higher.

EU Cyber-Security Directive

Who will the Directive apply to?

- ‘public administrations’
- ‘market operators’ which includes:

  e-commerce platforms
  Internet payment gateways
  social networks
  search engines
  cloud computing services
  application stores and
  the energy, transport, banking and health sectors.

- but... “non-exhaustive”

What does the Directive establish?

- Cyber-security Authority in each EU member state
- Co-operation Network
- Computer Emergency Response Team

Breach Notification Requirements – Get Ready

Which law will apply to you?

EU General Data Protection Regulation

- All companies processing and mishandling personal data fall into scope
- Current draft mandates notification to Supervisory Authorities within 72 hours
- Affected individuals must be notified only of breaches that are likely result in high risks for the freedom of individuals

Network and Information Security Directive

- Aim to regulate against cyber threats
- Operators must notify competent authority of incidents that have significant impact on services
- Energy, transport, banking industries, credit institutions, health, water industries, digital service providers will be subject to the law
- Most likely it will come in force in Q3 2017

Local data protection authorities imposing their own law

- From 1 Jan 2016 Netherlands: controllers are required to notify immediately local data protection authority of any security breaches
- Already existing laws in Austria, Germany, Norway and Russia and many regulators recommend voluntary notification


There may be trouble ahead
All site visitors please note that while there is:
• Moonlight
• Music
• Love
• Romance
It is advised that you:
• Face the music
• Dance
Pic.Twitter.com/chrisckmedia

Questions?

CharlesRussell Speechlys