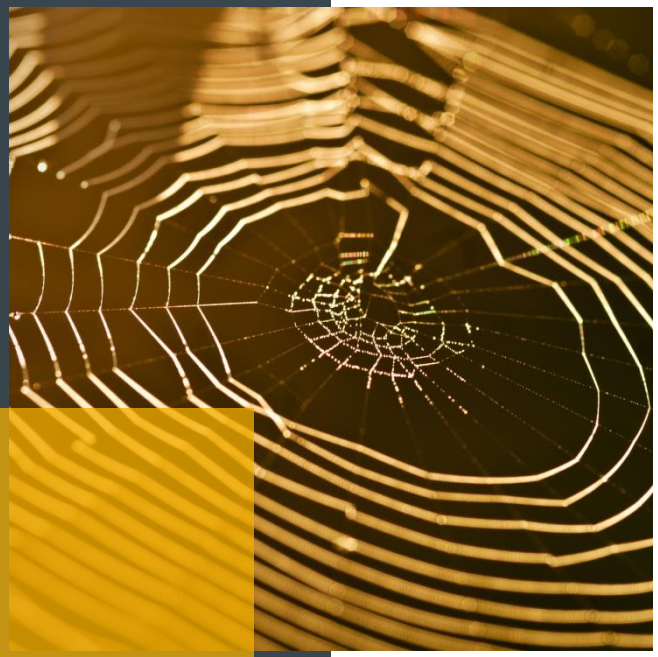
Simmons & Simmons

Data Protection Law
GDPR

Alex Brown



06 February 2018

Simmons & Simmons

Macro Overview

- Europe has a long history of protection of individuals' privacy and information
- The right to privacy is enshrined in the European Convention of Human Rights 1953
- 1981 – Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data
- 1995 – EU Data Protection Directive
- Privacy is increasingly important in sector specific regulation and also in the minds of European citizens
- 2016 - new EU Data Protection Regulation
- Data protection law is not an EU specific requirement (but the EU remains and wants to be the "high watermark")
- Cyber security – a challenge for businesses, Governments, law makers and regulators

Simmons & Simmons

Current EU Data Protection Regime

- EU Data Protection Directive implemented via local legislation in all EU Member States
  - a lack of truly harmonised law
  - different interpretations applied by data protection authorities / courts
  - multi-national companies face a different requirements and regulation in different countries
  - laws based on a Directive that is 20 years old

- The new EU Data Protection Regulation seeks to address these issues:
  - direct effect and no need for local implementing law
  - better co-ordination of data protection authorities and a “lead authority” for multi-national companies
  - to be passed in 2016 and come into effect in 2018

Current EU Data Protection Regime – when does the EU law apply?

- EU data protection law is not concerned with where the individual is or their citizenship. The EU data protection laws will apply if:
  - a company has an **establishment in the EU** (a company / branch / office)
  - **equipment in the EU** is processing personal data

- The Data Protection Regulation will extend the EU law to non-EU companies with no establishment in the EU but who are:
  - offering goods or services (for payment or for free) to individuals within the EU;
  - monitoring (i.e. profiling) individuals within the EU;
  - established in a place where EU law applies due to public international law, (i.e. a diplomatic mission or consular post) ; or
  - "data processors" – (i.e. non-EU companies who are processing personal data regarding individuals within the EU on behalf of another company).

Simmons & Simmons

Current EU Data Protection Regime – what does the EU law apply to?

- "Personal Data"
  - data (automatic equipment / "relevant filing system")
  - **relating** to a living individual
  - **identified** from that data
  - or from that data in combination with other data
- Only data relating to individuals (not company data)
- The information need not be confined to "personal life", it can include a person's "professional life"

Current EU Data Protection Regime – who does the EU law apply to?

- "Data Controller"
  - determines the **purposes** for which and the **manner** in which any personal data are processed
- "Data Processor"
  - processes data on behalf of a data controller
- You cannot be data controller and data processor in respect of the same data
- You can have more than one data controller in respect of the same data
- The importance of the difference - it is the duty of the data controller to comply with the DPA
- The Data Protection Regulation applies more obligations directly to data processors

Simmons & Simmons

Eight EU Data Protection Principles

- Personal data must be:
  - Fairly and lawfully processed
  - Processed for limited purposes
  - Adequate, relevant and not excessive
  - Kept accurate
  - Not kept longer than necessary
  - Processed in accordance with the data subject's rights
  - Kept secure
  - Not transferred to countries outside Europe without adequate protection

Eight EU Data Protection Principles

- Personal data must be:
  - **Fairly and lawfully processed**
  - Processed for limited purposes
  - Adequate, relevant and not excessive
  - Kept accurate
  - Not kept longer than necessary
  - **Processed in accordance with the data subject's rights**
  - **Kept secure**
  - **Not transferred to countries outside Europe without adequate protection**

First Data Protection Principle: fair and lawful processing

- Personal data must be processed fairly and lawfully – that means:
  - have a **justification / legal basis** for the processing – there is a list in the legislation
  - tell individuals what is being done with their data
- Justifications often used:
  - consent (active and informed)
  - performance of contract
  - compliance with legal obligation
  - legitimate interests
  - sensitive personal data – explicit consent / employment law obligation
- Information requirement is separate from justification requirement
  - identity of data controller
  - purpose of processing,
  - “fair” information

First Data Protection Principle: Consents and Notices (Regulation)

- Data controller has burden of proving that the data subject has given consent to the processing
- Consent not valid if there is a “significant imbalance of power” (e.g. employer / employee relationship)
- Information to be provided includes:
  - data controller’s identity and contact details (including representative and data protection officer)
  - purposes and legal basis for processing
  - period for which the data will be stored (or criteria to determine it)
  - existence of the rights to access, to rectify, to erasure, to object to processing or to obtain the data
  - right to lodge a complaint with the national data protection authority
  - recipient or categories of recipients to whom the data will be disclosed.
  - intention to transfer the data subject’s personal data overseas

Internal Processes under the Regulation

- Under current Directive – “outputs based” regulation - no established processes to be followed to achieve compliance
- Under Regulation, more detailed requirements about how organisations must achieve compliance:
  - Data Protection Officers (for some organisations)
  - transparent policies and communication
  - implementation of mechanisms, the observance of time limits for erasure and of review of the need for storage of personal data
  - policies and demonstrable measures in relation to compliance with the Regulation
  - risk assessments (for specific “risky” situations) and privacy impact assessments
  - “privacy by design” / “privacy by default”

Simmons & Simmons

Sixth Data Protection Principle: individuals' rights

- Individuals are given various rights under EU data protection law:
  - right to access their data
  - right to prevent processing causing damage or distress
  - right to prevent processing for direct marketing
  - rights in relation to automated decision making
  - right to require an organisation to rectify, block, erase or destroy personal data
  - right to compensation
- These rights are extended under the Regulation:
  - "right to be forgotten"
  - right to "data portability"

Seventh Data Protection Principle: Data Security – Data Controllers

- The controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access,
- **Technical and organisational** security – it is not just an IT problem
- **"Appropriate"** - having regard to the state of technology and cost, security must be appropriate to:
  - the harm that might result from such unauthorised or unlawful processing or accidental loss / destruction / damage
  - the nature of the data
- Reasonable steps to ensure the reliability of employees who have access to data

Seventh Data Protection Principle: Data Security – Data Processors

- Contracts with data processors
- Requirements for data controllers to remain compliant with seventh principle
  - data controller "guarantees" regarding technical and organisational security
  - data controller takes reasonable steps to ensure compliance with measures
- Data controller not regarded as seventh principle compliant unless
  - contract with data processor is evidenced in writing
  - data processor is only to act on instructions of data controller
  - contract requires data processor to comply with security obligations equivalent to those of seventh principle

Seventh Data Protection Principle: Data Security (Regulation)

- Risk-based approach to the implementation of security measures to protect against loss or unauthorised disclosure of personal data
- Data controllers and data processors must implement appropriate security measures and implement a security policy
- **Breach notification** –
  - new, mandatory requirement for data controllers to notify national data protection authorities of security breaches "without undue delay"
  - data controllers will be required to notify affected individuals in wide-ranging circumstances
- Data controllers will have to keep **records of security breaches**
- Forthcoming cyber security Directive and more regulation generally on cyber security

Eighth Data Protection Principle: Transfers of data outside EU

- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data
- This rule comes into play if you have an entity within the EU transferring data outside the EU
- What is “transfer”?
  - wording of the Directive points to substantive processing in the third country
  - Information Commissioner’s guidance - “transfer” is not the same as “transmit” / must be some substantive processing of the data in the third country

Eighth Data Protection Principle: Transfers of data outside EU

- Three options for compliant transfers:
  - EU findings of adequate protection for data
  - Creating adequate protection for data
  - Rely on an exemption
- The Regulation does not alter the data transfer requirements
- EU finding of adequacy
  - **Approved countries**: the EU Commission has so far recognized **Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay** as providing adequate protection.
  - **USA: Safe Harbor**
    - 2015 - declared invalid by European Court of Justice
    - “Privacy Shield”

Eighth Data Protection Principle: Transfers of data outside EU

- Creating adequate protection for data
  - EU approved data transfer agreements
  - Binding corporate rules
- Data transfer agreements
  - controller → controller (two versions)
  - controller → processor
  - agreements are **standard form** – you cannot alter them (other than to fill the gaps)
  - the agreements contractually bind the recipient to adopting EU standards of data protection
  - individuals have the right to see and enforce the data transfer agreements
  - EU based controllers responsible for what happens to the data outside the EU

Eighth Data Protection Principle: Transfers of data outside EU

- Creating adequate protection for data
  - EU approved data transfer agreements
  - Binding corporate rules
- Binding Corporate Rules
  - an instrument to freely transfer personal data within a company worldwide
  - can be used by controllers or processors
  - in theory a simpler mechanism for compliance. In practice can be expensive and costly to put in place
  - submission to “lead authority” including:
    - description of data flows/processing
    - policies/agreements making up the BCR
    - description of legally binding effect – internally and externally
  - lead authority supposed to co-ordinate approvals/comments from other national authorities

Eighth Data Protection Principle: Transfers of data outside EU

- Exemptions
  - **Consent** of data subject
  - Necessary for the **performance of a contract** between the individual and the data controller
  - Necessary or legally required on important **public interest grounds** or for the establishment, exercise or defence of legal claims
  - Protect a **vital interest** of the individual
  - The transfer is made from a register which according to laws or regulations is intended to provide **information to the public**
- Exceptions should be interpreted restrictively (for example consent: unambiguous, specific and informed / not to be used for regular transfers, only on an exceptional basis)

Enforcement

- Under the current EU Directive:
  - powers to issue administrative fines – around £300,000 - £500,000 maximum
  - criminal offences (for companies and individuals)
  - rights for authorities (e.g. audit / investigation rights)
- Under the Regulation
  - Fines – depending on breach – greater of:
    - **€10m or 2% of annual worldwide turnover**
    - **€20m or 4% of annual worldwide turnover**
  - Enhanced powers for authorities including:
    - impose a temporary or permanent **ban on data processing**
    - **suspend data flows** outside Europe

Simmons & Simmons

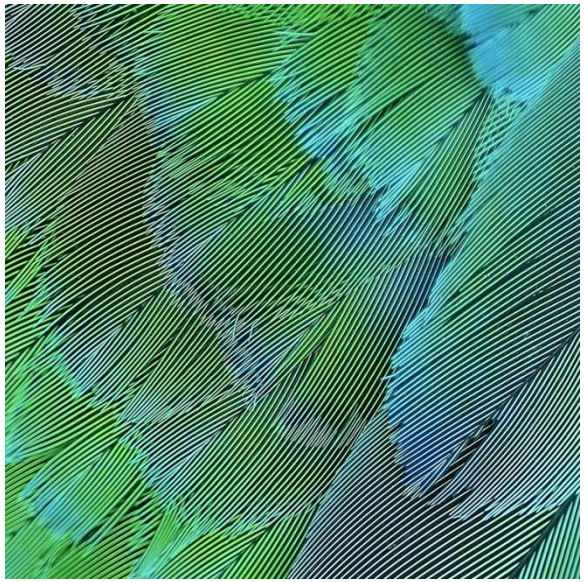
Questions?

simmons-simmons.com
elexica.com
@Simmons_LLP

Simmons & Simmons elexica

Elexica Resources Relevant to this Session

GDPR



- Visit our microsite on elexica for an overview of what you need to know about the EU Data Protection Regulation: Read here
- Visit the Events page for forthcoming seminars and training days and the Training page for video recordings, podcasts and slides

Request a demo
Contact elexica@simmons-simmons.com or speak to your usual Simmons contact to find out more.

Simmons & Simmons

simmons-simmons.com
elexica.com