SK | STONE KING

# Debunking GDPR– what do you need to know to be compliant?

Vicki Bowles

6 March 2018

# How does GDPR work?

# 4 Steps to Compliance

- Understand the law
- Audit the information you have
- Check policies and procedures
- Train your staff

# Understand the Law

- What is Personal Data?
- Data Protection Principles Mark II
  - Lawful grounds for processing
- Privacy Notices
- Processor Contracts
- Risky Processing
- Individual Rights
- International Transfers
- Policies

# What is Personal Data?

- Reminder:
  - Applies to all personal information of living individuals
    - Identifies an individual:
      - Susan Smith not,
      - Vicki Bowles possibly,
      - Lady Karen Brady definitely.
    - Includes all people – staff, volunteers, beneficiaries, you…
  - Applies whatever you are doing – collecting, using, deleting and everything in between

# The Data Protection Principles Mark II

**Whenever** you deal with Personal Data you must…

1. Deal with it lawfully, fairly and in a transparent manner
2. Collect for specific purpose (s) and not use in a way incompatible with that purpose (some exceptions)
3. Ensure what you have is adequate, relevant, limited to what is necessary
4. Ensure what you have is accurate and kept up to date – erase or rectify without delay if not
5. Ensure that you have is kept in identifiable form no longer than necessary
6. Ensure appropriate security, including protection against unauthorized or unlawful processing, and accidental loss or damage

# First Principle

# Fair

- Look at the circumstances when you obtained the information
  - What would be a reasonable use in those circumstances?
- What is the connection between the use for which you collected the information, and the use to which you want to put it?

# Transparent

- How obvious is this use?
- What have you told individuals about what you intend doing with their information?
- What's in your Privacy Notice?
- What's in your ICO register entry (if you have one)

# Lawful

- With consent
- Necessary for performance of contract to which data subject is party or necessary to take steps prior to entering into a contract at request of data subject
- Necessary for compliance with legal obligation
- Necessary to protect vital interests of subject or another
- Necessary for performance of task carried out in public interest or in exercise of official authority vested in controller
- Necessary for legitimate interests of controller or third party, except where overridden by interests or fundamental rights and freedoms of data subject

# Consent means…

- Art 4 (11)
  - "*freely given, specific, informed and unambiguous indication of data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data related to him or her*"
- Art 7:
  - *Demonstrable*
  - *If written declaration containing other matters – must be clearly distinguishable, intelligible and easily accessible form, using clear and plain language – or it's not binding*
  - *Right to withdraw at any time*
  - *When deciding if freely given, have UTMOST regard to whether consent is conditional for provision of service/performance of contract where personal data itself not necessary for provision of that service/contract*

# Why is this important?

- Because you have to tell people the legal basis on which you're holding/using their information when you collect it…

# Privacy Notices

- Identity and contact details of: Controller, and any DPO;
- The purposes for which information is being collected;
- The legal basis for use of information:
  - If consent – mention withdrawal;
  - If necessary for legitimate interests – detail what those interests are;
  - If statutory requirement or contract – whether or not obligatory and consequences of not providing
- Recipients/categories of recipients;
- Details of safeguards if outside EEA;
- Retention period or criteria used to determine the period;
- The existence of the rights to access information, rectification, erasure, object to processing, and data portability;
- The right to complain to the ICO;

# Data Processors

- Third party acting under your instruction and control when doing something with personal data for you
- Should already have a written agreement in place, but additional requirements
- Check IT contracts particularly
- Add in:
  - Duty of confidentiality on staff;
  - Subcontract with Controller permission;
  - Assist Controller with subject rights and security;
  - Return or delete at end – controller's choice;
  - Make info about activity available to controller.

# High Risk Processing

- Certain circumstances require risk assessment
- Any high risk processing
- Identify risks and mitigation factors

# Individual Rights

- Subject Access – 30 days
- Rectification
- Erasure
- Restriction
- Portability

# International Transfers

- Prohibited unless you can show data is protected when it leaves. Various ways of doing this:
  - Country has an adequacy decision (see http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)
    - Currently Andorra, Argentina, Canada (commercial orgs only), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay
  - Transfer is subject to a Code of Conduct that provides for a binding and enforceable commitment from the third country, that has been approved by the ICO
  - Agreement between organisations that contains approved clauses

# Transfers Continued

- Explicit consent – with full understanding by individual of risks
- Necessary for a contract:
  - With individual as party
  - Pre contract at individual's request
  - With another, but in interests of individual
- Public interest grounds that are recognised in law (possibly charitable?)
- Establishing, exercising or defending legal claims
- Protect vital interests of individual where physically or mentally incapable of giving consent
- Necessary for compelling legitimate interests BUT:
  - Must not be repetitive and with a limited number of individuals
  - Must be a suitable agreement in place with safeguards
  - Inform the ICO and the individuals

# Policies

- REQUIRED
  - Data Breach
  - Data Retention
  - Use of sensitive information for employment
  - Use of DBS information
- OPTIONAL
  - General data protection
  - ICT
  - BYOD

# Questions?