womblebonddickinson.com

WOMBLE BOND DICKINSON

Schools North East Conference 2018

GDPR: 5 things you need to know!

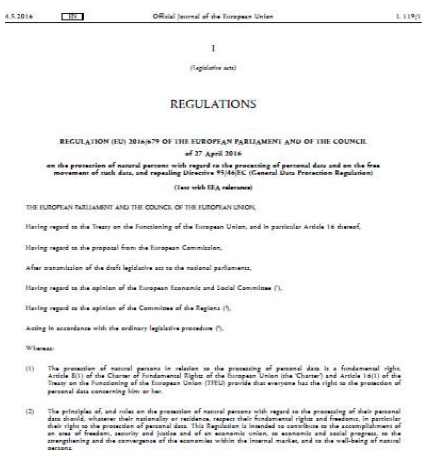
Jackie Gray, Partner

16 January 2018

GDPR - 5 things you need to know!

1. What is the GDPR?
2. What is the legal framework and timetable?
3. What are the key changes and what do we need to do about them?
4. What else do we need to do?
5. Where can we find out more and get help?

1. What is the GDPR?



4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

- Replaces current Data Protection Directive from 25 May 2018
- Single data protection law across Europe
- Provides enhanced rights for individuals
- Greater and more prescriptive obligations on organisations processing personal data
- More serious consequences for non-compliance
- "Evolution, not Revolution"

2. What is the legal framework & timetable?

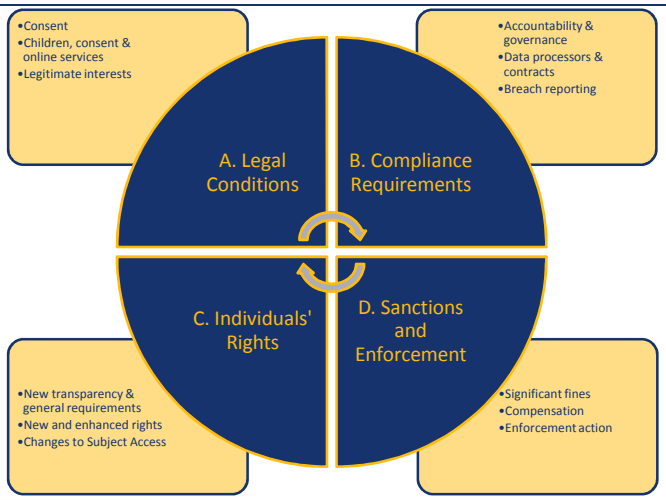
Data Protection

- The Data Protection Act 1998 (**DPA**) - applies until 24 May 2018
- General Data Protection Regulation (**GDPR**) - applies from **25 May 2018**
- New Data Protection Act 2018 (currently the Data Protection Bill) – applies from **25 May 2018**:
  - Brexit proofs the GDPR
  - Supplements the GDPR

Electronic Direct Marketing

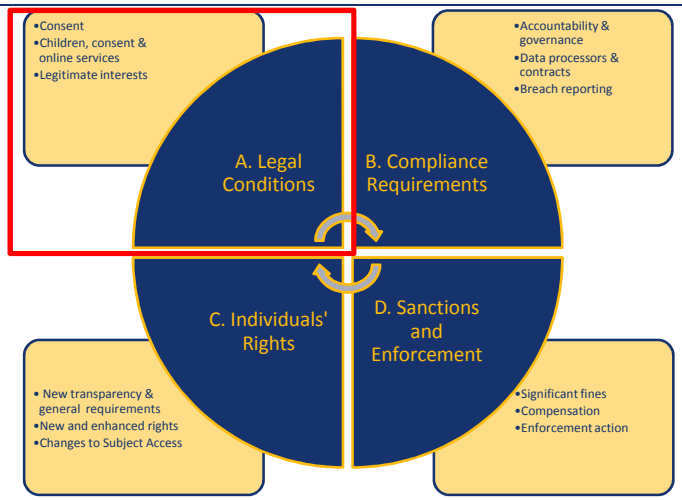
- Privacy and Electronic Communications Regulations 2003 (**PECR**) implement the ePrivacy Regulation – apply until 24 May 2018?
- New draft ePrivacy Regulation – intended to apply from 25 May 2018 but…….

3. What are the key changes and what do we need to do about them?



WOMBLE BOND DICKINSON

3. What are the key changes? A – Legal Conditions



WOMBLE BOND DICKINSON

A: Legal Conditions: New legal conditions and changes to legitimate interests condition

- For processing to be lawful there must be a lawful condition of processing in the GDPR which covers the processing – the most appropriate condition will depend on the purposes of the processing.
  - Different processing conditions apply to (i)' personal data', (ii) 'special categories of personal data' and (iii) 'criminal conviction data'
  - NEW - 'Special categories of personal data' now includes biometric data for purposes of identification eg biometric access control data
- GDPR still permits processing of personal data where it is necessary for the purposes of legitimate interests pursued by the controller or by a third party but NOT for processing carried out by public authorities in the performance of their tasks. This includes academies and maintained schools
- There is however a condition permitting processing of personal data where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority. Under DPA18, this includes where processing is necessary for the exercise of a statutory function.

A: Legal Conditions - Consent

Consent

- *Consent must be freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data*
  - Positive opt-in required
  - Separate consents for different purposes
  - Specific and granular; clear and concise
  - Capable of and easy to withdraw
  - Evidence of consents required
- Consent to process "special categories" of personal data must be explicit

A: Legal Conditions – Children & Consent

Children's consent & online services

- GDPR contains provisions intended to enhance the protection of children's personal data
- Where you directly offer a child online services involving the processing of their personal data and the basis of this is their consent, they must be 13 or over, otherwise you will need to obtain consent from the person with parental responsibility
- Any other processing: current rules continue to apply:
  - Consent based on a child's capacity to understand
  - Age 12 in Scotland and therefore a starting point

Digital Age

13

Otherwise

12*

WOMBLE BOND DICKINSON

A: Legal Conditions: what do we need to do? Consider the following:

Consents

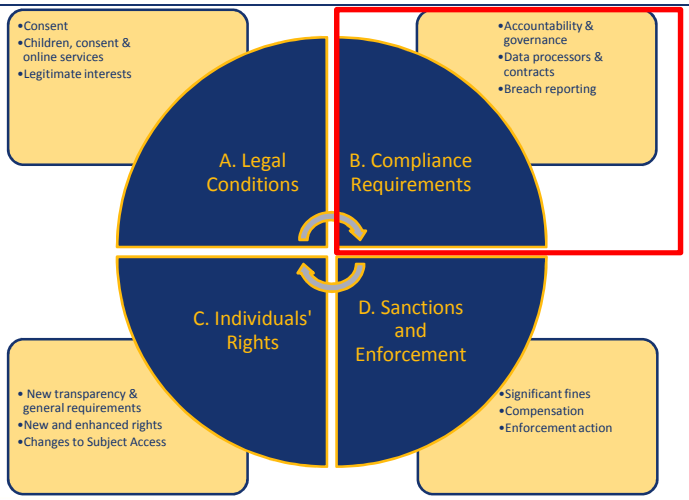
- When do you currently rely on it and how do you obtain it?
- Do you directly provide any online services to children?
- Is there another lawful basis for processing instead of consent?
- If not, review and change how consent is obtained to be compliant & obtain parental consents if required

Other legal basis

- What other legal basis do you rely on to process personal data?
- Identify different purposes of processing and legal basis for each
  - Needed for record keeping
  - Needed for privacy notices

WOMBLE BOND DICKINSON

3. What are the key changes?
B: Compliance Requirements



WOMBLE BOND DICKINSON

B: Compliance Requirements – Accountability & Governance

Accountability & Governance

- New Accountability Principle which requires you as data controllers to be responsible for and to be able to demonstrate compliance with the data processing principles
- This means keeping detailed records/documentation that may need to be presented to the ICO on request
- This principle runs through the GDPR and is also reflected in a number of specific additional accountability & governance requirements

WOMBLE BOND DICKINSON

B: Compliance Requirements – Accountability & Governance (2)

Art	Requirement
24	Controller must implement appropriate technical/organisational measures to ensure/demonstrate compliance – **including DP policies**
25	Data protection by **design & by default**
30	Written **records** of processing activity must be kept, including: • The purpose of processing • The description of data subjects / personal data • The categories of recipients • The details of transfers o/s the EEA • The envisaged retention periods • A description of security measures and must be made available to regulator on request.

B: Compliance Requirements – Accountability & Governance (3)

Art	Requirement
35	Privacy Impact Assessments (**PIAs**) for "high risk" processing activities
36	Prior **consultation with the regulator** for certain high risk processing activities (as informed by the PIA)
37-39	Requirement for, tasks and duties of, a **data protection officer (DPO)** **All public authorities must appoint a DPO on basis of their professional qualities and expert knowledge of data protection law and practice**

B: Compliance Requirements - Data Processors & Contracts

- Data processors now have direct responsibility for certain areas of compliance under GDPR
- Contracts with data processors must contain specific contractual terms required by the GDPR
  - These are new requirements
  - It is the responsibility of the data controller to make sure these are in place
  - Requirements apply to existing and new contracts from May 2018
- Where processing of personal data is processed outside the EEA, additional legal requirements must be met, including record keeping requirements

WOMBLE BOND DICKINSON

B: Compliance Requirements – Data processing jointly with other Data Controllers

- Joint data controllers
  - *"two or more controllers who jointly determine the purpose and means of processing"*
- New obligations imposed on joint data controllers:
  - Need to determine their respective responsibilities in an "arrangement" ie data sharing agreement/MOU
  - The essence of the arrangement must be made available to individuals ie summary or copy
  - Individuals may exercise their rights against each data controller
- May apply to certain data sharing arrangements you currently have in place

WOMBLE BOND DICKINSON

B: Compliance Requirements – What is a personal data breach?

- "…*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*"

© CarmeloWalsh.com

B: Compliance Requirements - Breach Reporting

Personal data breach (all)

Document data breaches

Breach likely to result in risk to rights and freedoms of individuals

Notify regulator without undue delay and (where feasible) within 72 hours of becoming aware

If not within 72 hours, need to explain reasons

Breach likely to result in high risk to rights & freedoms of individuals

Notify data subjects without undue delay, unless…

- Personal data was protected

- Controller has taken steps which ensure high risk is unlikely

- Disproportionate effort

Data processor must also notify the data controller without undue delay after becoming aware of any personal data breach.

B: Compliance Requirements - what do we need to do? Consider the following:

Accountability & Governance

- Review and update policies & procedures
- Provide staff training on changes
- Appoint and train DPO
- ID what records you are required to keep and produce them
- Produce template PIA process and report
- Risk & reporting process to SMT and Governors

Data Processors & Contracts

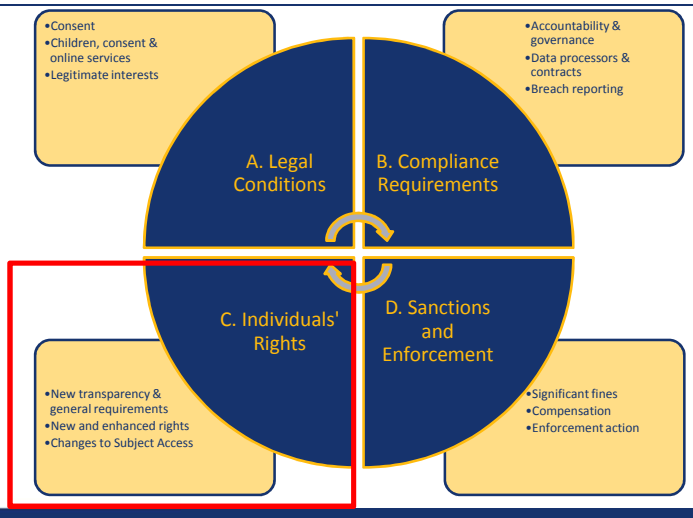
- Are you a data processor for someone else?
- Your suppliers now have certain legal obligations – beware of price increases and changes
- Identify, review and update existing DP contracts to be compliant
- Identify overseas processing and ensure this is compliant
- Ensure new contracts have required clauses in them
- Ensure supplier due diligence includes GDPR requirements

Data Breach Reporting & Management

- Update policies and procedure to reflect requirements
- Put in place a breach response plan, mapping out roles / responsibilities etc
- Carry out mock breach response exercises
- Put in place measures to secure "vulnerable data" – encryption

WOMBLE BOND DICKINSON

3. What are the key changes? C: Individuals' rights



WOMBLE BOND DICKINSON

C: Individuals Rights – Transparency requirements & general requirements, including SARs

- Information & communications regarding an individual's rights must be concise, transparent, intelligible, accessible and in clear and plain language, particularly if addressed to a child
- Rights can all be exercised free of charge (no more £10 fees for SARs)
  - unless manifestly unfounded or excessive (includes repeat requests) when they can be refused or a reasonable fee can be charged (to be set by Regulations)
- Requests must be responded to promptly and, generally, within 1 month (28-31 days)
  - Extendable by 2 further months if necessary due to complexity/number of requests
- If a request is made electronically, information to be provided by electronic means where possible – will apply to SARs

C: Individuals Rights – Privacy Notices

Privacy notices must:

- be concise, transparent, intelligible, easily accessible form, use clear and plain language, particularly for information addressed specifically to a child
- be provided in writing, or by other means, including where appropriate by electronic means and where requested, be provided orally
- contain additional required information (including legal conditions for processing & retention periods) when you:
  - collect personal data from the individual
  - when you obtain personal data from a third party

C: Individuals Rights – New & Enhanced Rights, subject to exemptions

Art	Right
15	Right of access to personal data - ENHANCED
16	Right of rectification - ENHANCED
17	Right to erasure / to be forgotten - NEW
18	Right to restrict processing - NEW
19	3rd party notification of rectification, erasure or restriction - NEW
20	Right to data portability - NEW
21	Right to object – including right to object to direct marketing and profiling related to direct marketing - ENHANCED
22	Automated decision making - ENHANCED

EXEMPTIONS GDPR & DPA 18

C: Individuals' rights- what do we need to do? Consider the following:

SARs

- Review SAR procedure and update to address changes, including shorter timescales
- Update guidance to reflect new exemptions

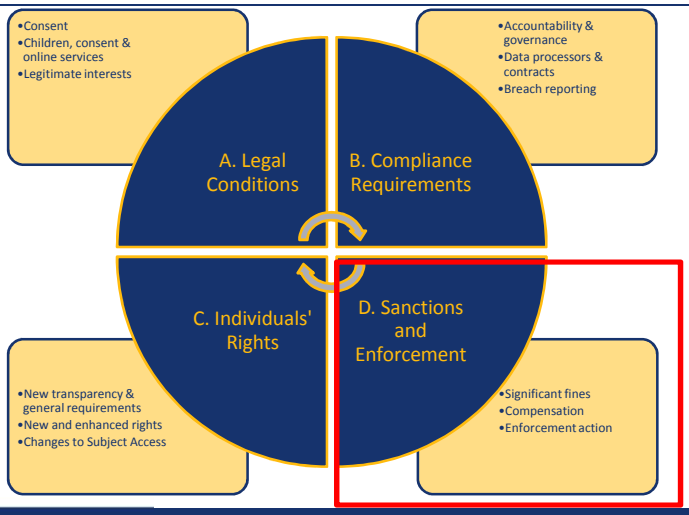
Privacy Policies

- Identify different purposes & conditions of processing
- Need to tailor to your audience, including children
- Need to identify retention periods
- Consider layering, ICONs, animations & videos

Other Rights

- Identify which rights apply to which data
- Put in place policies & procedures for dealing with new rights and amend to reflect changes to existing rights
- Build PIAs into new projects procedures etc
- Consider system changes

3. What are the key changes?
D: Sanctions & enforcement



WOMBLE BOND DICKINSON

D: Sanctions & enforcement - ICO enforcement powers & criminal offences

- ICO Powers:
  - Information notices & undertakings
  - Enforcement notices and 'stop now' orders
  - ICO mandatory audits – now extended to all organisations
  - Monetary penalty notices
- Criminal offences including new offences:
  - Knowingly/recklessly re-identifying anonymised data without consent of the data controller
  - Retaining data without consent of the data controller
  - Alter, deface, block, erase or conceal data to prevent disclosure in response to a SAR

WOMBLE BOND DICKINSON

D: Sanctions & enforcement – Fines, or the Big Stick!

There are two tiers of fines which apply to both controllers and processors:

- **Tier 1**: up to **2%** of annual worldwide turnover or **€10,000,000 (£8.5M)** (whichever is the higher) eg
  - Failure to comply with data processor requirements
  - Failure to maintain required written records
- **Tier 2**: up to **4%** of annual worldwide turnover or **€20,000,000 (£17M)** (whichever is the higher) eg
  - Failure to comply with data protection principles
  - Failure to comply with an individual's rights, including SARs

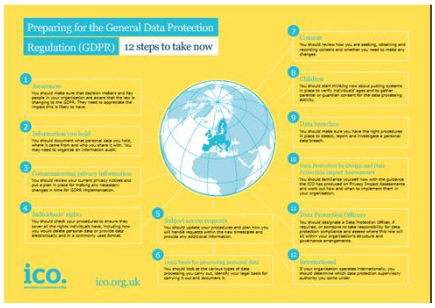
D: Sanctions & enforcement – Compensation rights

- Any person who has suffered material or non-material damage as a result of a breach of the GDPR has the right to receive compensation from the controller or processor for the damage suffered
  - Not limited in amount
  - Includes distress claims
  - Claims can also be brought by certain representative organisations on behalf of individuals
- Increase in risk to organisations
- May be mitigated through insurance eg cyber insurance

4. What else do we need to do? Put in place and implement a GDPR project - AAA

- **Audit: your use of personal information**
  - What do you hold? How do you use it?
  - Who do you share it with? Why?
  - How long do you keep it?
  - Complete a data map to inform compliance including recordkeeping, privacy notices, individuals' rights, data processing, data sharing & security
- **Analyse: your use of personal information & governance procedures**
  - Identify gaps in compliance (gap analysis)
  - Prepare a plan to address gaps
- **Address:**
  - Implement plan

5. Where can we get help & more information?



Information Commissioner's Office (ICO)

- GDPR Guide
- GDPR Blog
- GDPR self-assessment checklists
- GDPR FAQs for education sector

www.ico.org.uk

Womble Bond Dickinson!
E: jackie.gray@wbd-uk.com
E: kevin.robertson@wbd-uk.com

www.womblebonddickinson.com

Questions

Jackie Gray
Partner

T: 0113 290 4432
E: Jackie.gray@wbd-uk.com

WOMBLE BOND DICKINSON