7 March 2018

Introduction to GDPR

Melanie Carter
Alistair Williams

Bates Wells Braithwaite

Overview

Bates Wells Braithwaite

Introduction

“The General Data Protection Regulation builds on the previous legislation: but provides more protections for consumers, and more privacy considerations for organisations. It brings a more 21st century approach to the processing of personal data. And it puts an onus on [organisations] to change their entire ethos to data protection …. The message about GDPR is continuity and change.

There’s a lot in the GDPR you’ll recognise from the current law, but make no mistake, this one’s a game changer for everyone.”

Elizabeth Denham, Information Commissioner, 17 January 2017

Bates Wells Braithwaite

What will we be covering today?

- Overview and key concepts
- Data protection principles
- Data processors
- Data subjects' rights
- Transfers
- Accountability and governance
- Security and breaches
- Non compliance
- Workshop
- Tips

Bates Wells Braithwaite

Overview

- EU Regulation – no need for implementing legislation (but N.B. Data Protection Bill)
- Brexit will not affect commencement – GDPR here to stay
- GDPR comes into force 25 May 2018, no transitional period
- GDPR applies to processing carried out by organisations operating within the EU/to organisations outside the EU offering goods or services to individuals in the EU
- Separate plans for e-Privacy Regulation (covering electronic direct marketing, cookies etc.)

Bates Wells Braithwaite

Recap of key concepts

Bates Wells Braithwaite

Key concepts

- Applies to **data controllers** (who control how and why personal data is processed) and **data processors** (who act on the controller's behalf)
  - New requirements on data processors (previous regime did not apply to them)
- Applies in respect of **personal data** – essentially any information relating to an identifiable natural person
  - Key questions: (a) can an individual be identified from the data (and other available information), and (b) does the data "relate to" that individual?
- Applies to **data processing** - any operation performed on personal data (collection, storage, disclosure etc.)

Bates Wells Braithwaite

How do BDIA members use personal data?

Employee data

Information on customer/supplier contacts

Personal data for marketing

Managing patient data on behalf of dental practice?

Bates Wells Braithwaite

Data protection principles

Bates Wells Braithwaite

GDPR: Principles (art 5)

Personal data shall be:

1. Processed fairly and lawfully and in a transparent manner (‘lawfulness, fairness and transparency’)
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’)
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)
4. accurate and, where necessary, up to date (‘accuracy’)
5. not to be kept longer than necessary (‘storage limitation’)
6. Processed in a manner that ensures appropriate security (‘integrity and confidentiality’)

Bates Wells Braithwaite

GDPR Basis for processing (art 6)

To be lawful, there must a valid basis for processing:

- Consent (new requirements) 

- Performance of a contract with data subject
- Compliance with a legal obligation to which data controller is subject
- Vital interests
- Public interest
- Legitimate interests, unless outweighed by interests/rights/freedoms of data subject (not for public authorities - new) 

Do you know what personal data you are processing and your legal basis for doing so?

Bates Wells Braithwaite

Special categories of (ie sensitive) personal data

racial or ethnic origin	political opinions	religious or philosophical beliefs
trade union membership	genetic data NEW	biometric data (for ID purposes) NEW
health	sex life or sexual orientation	**NB** – processing of personal data on criminal convictions and offences also restricted

Bates Wells Braithwaite

Processing special categories of personal data

Processing special categories prohibited **unless**:

- Data subject gives explicit consent
- Necessary for employment or social security/protection law*
- Necessary to protect vital interests
- Processing with safeguards by not-for-profit body with political, philosophical, religious or trade union aim which relates solely to members (no disclosure outside of body without consent)
- Data made public by data subject
- Necessary for legal claims
- Necessary for reasons of substantial public interest*
- Health and social care*
- Public health*
- Archiving, research and statistics*

* = additional conditions/safeguards in Data Protection Bill

Bates Wells Braithwaite

Legitimate Interests (1)

- What is the ‘Legitimate Interests’ condition?

Article 6(1)(f) GDPR:

“Processing is necessary for the purposes of the legitimate interest pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

Bates Wells Braithwaite

Legitimate Interests (2)

- ICO sets out a three-stage "balancing test" which must be used when assessing whether it is possible to rely on the legitimate interests to process data:

- *What is your legitimate interest or that of a third party?*
- *Is the processing of the personal information <u>necessary</u> to pursue that legitimate interest?*
- *Even if it is, would the processing affect the rights and freedoms or legitimate interests of the individual(s) in such a way and to such an extent that it is unjustified?*

- Should record the balancing exercise ("legitimate interest assessment").

Bates Wells Braithwaite

New standard of consent

Consent must be:

- freely given
- specific
- informed
- an unambiguous indication of the data subject's wishes
- distinguishable from other matters if in a statement

Requires statement or clear affirmative action agreeing to processing

Silence, pre-ticked boxes or inactivity do not establish consent

Bates Wells Braithwaite

Relying on consent

Is consent the appropriate basis?

- ICO draft guidance: consent inappropriate where no genuine choice (eg position of power, such as employer) or consent is a precondition of service

Nature of existing consent

Withdrawal of consent as easy as giving it

Record-keeping

Bates Wells Braithwaite

Privacy Notices (transparency)

Generally more onerous requirements – privacy statements or other communications with data subject must include:

- Identity and contact details of data controller/ DPO
- Purposes of the processing
- Legal basis for processing (e.g. legitimate interests)
- Recipient/categories of recipient of the personal data
- Transfer of data outside EEA
- How long data will be held for
- Individuals' rights
- Right to lodge a complaint with ICO
- Existence of automatic decision making

Bates Wells Braithwaite

ICO guidance

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	✓	✓

Bates Wells Braithwaite

Data processors

Bates Wells Braithwaite

Key concepts recap – quiz (i)

1. Which of the following are data controllers and data processors?

- An external company providing payroll services to a BDIA member
- A marketing company sending marketing materials on behalf of a BDIA member
- Dental Practice A is closing so transfers its patient lists to Dental Practice B
- A BDIA member gives the contact details for individuals from its customers to a research company and asks it to conduct a satisfaction survey

Bates Wells Braithwaite

Key concepts recap - quiz (ii)

2. Is the (i) BDIA member and (ii) the dental practice a data controller, data processor or neither?

a) A BDIA member sells patient record management software to a dental practice. The dental practice controls what personal data is recorded and how.

b) What if the company offers cloud storage with the software?

c) A dental practice sends a scan of a patient's mouth to an external dental laboratory to order a custom made dental appliance, using a BDIA member's equipment

3. How could the dental practice in (c) avoid transferring personal data?

Bates Wells Braithwaite

What will change under GDPR? In a nutshell

- Some aspects of the GDPR will apply to processors (such as payroll providers and software companies) directly e.g. implement appropriate security measures, appoint DPOs, keep records of processing

- Data controllers will be required to seek guarantees (Article 28(1)) which indirectly requires processors to comply with GDPR

- Expands what needs to go into contracts with data processors

Bates Wells Braithwaite

What needs to go into contracts under GDPR (1)

- Description of:
  - scope, nature and purpose of processing
  - duration of processing
  - types of personal data and categories of data subject

- Processor must:
  - only process pursuant to controller's instructions (subject to contravening obligations under EU or national law)
  - ensure staff are subject to duty of confidence
  - keep data secure
  - assist controllers to comply with requests to exercise rights by data subjects
  - sub-processor must only be used with consent of controller
  - ensure obligations are passed onto any sub-processor in written contract (Article 28(4))

Bates Wells Braithwaite

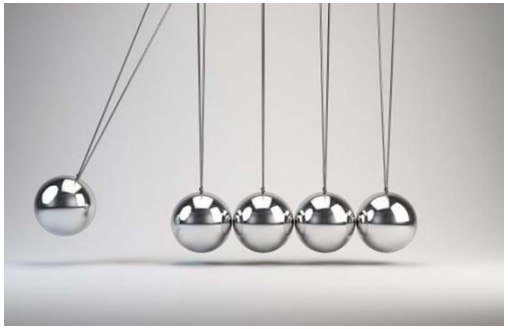
What needs to go into contracts under GDPR? (2)

- Processor must:
  - assist data controller to carry out privacy impact assessment, managing breaches and dealing with ICO (Article 28(3)(f))
  - return or delete personal data at the end of the agreement (unless they need to keep it to comply (with law)
  - demonstrate its compliance with these obligations and allow controller to carry out audits (Article 28(3)(h))

Bates Wells Braithwaite

What will be the practical implications of these changes? (1)

- Will need to revisit data processing agreements
  - No transitional provisions so start updating contracts now if you haven't already
- Important for both controllers and processors
- Processors may seek cross indemnities against losses they suffer as a result of the actions of data controllers
- Enhanced due diligence checks



Bates Wells Braithwaite

Data subjects’ rights

Bates Wells Braithwaite

New <u>access rights</u> - Greater rights are given to individuals, including rights of erasure, protection against profiling, and a right of data portability.

Bates Wells Braithwaite

Subject rights (1)

- Right to be **informed** (transparency information) (Arts 13, 14)

- Right of **access** (i.e. subject access request) (Art 15):
  - without undue delay and within **one month** (extendable by two where complex/numerous)
  - **No longer** permissible to charge a fee (unless manifestly unfounded/excessive)

- Right to **rectification** (where information is inaccurate or incomplete), including liaison with third parties to whom you have disclosed the data (Art 16)

Bates Wells Braithwaite

Subject rights (2)

- Right to **restrict processing** (Art 18)
- Right to **object** (Art 21)
- Rights on **automated decision making/ profiling** (Art 22)
- Right to **data portability** (Art 20)
- Right to **erasure** ('right to be forgotten') (Art 17)
  - personal data no longer necessary
  - consent is withdrawn
  - data subject objects

TIP – Review policies against new rights, particularly how subject access requests and requests to be forgotten are dealt with

Bates Wells Braithwaite

Transfers

Bates Wells Braithwaite

International transfers of data (Articles 44-50)

Similar rules to the DPA apply to all organisations:.

- There must be adequate **safeguards** in place for transfers to countries outside the EEA.
- Some countries deemed safe (**limited list**)
- Transfers to the USA may be permitted if it is to an organisation which has **privacy shield status**
- Transfers can take place where **model contract clauses** are used
- Transfers permitted where needed to comply with a **contract**
- New provisions under GDPR permit transfers where they are under an approved **code of conduct**, approved **certification mechanism**, or approved **contract clauses**.
- GDPR also covers onward transfers to **third countries**

Bates Wells Braithwaite

Transfers outside of the EEA

- Possible examples of transfers:
  - Hosting personal data outside the EEA
  - Using IT companies based outside of EEA/server based outside of EEA who backup server data/cloud storage
  - International subsidiaries/partners - sharing or allowing access to personal data
- Transfers prohibited unless:
  - Adequacy decision, eg EU-U.S. Privacy Shield
  - Appropriate safeguards, eg model clauses
  - Derogations, eg explicit consent

Bates Wells Braithwaite

Accountability and governance

Bates Wells Braithwaite

Accountability

- New principle requires demonstration of compliance with DPP (art 5(2))
- ICO registration requirement replaced by keeping own (detailed) record of processing activities
- Data controllers will still be required to pay a fee to the ICO
- New (explicit) requirement to implement appropriate technical and organisational measures to implement DPP (privacy by design)

Bates Wells Braithwaite

Privacy Impact Assessment (1)

What is a Privacy Impact Assessment?

- Tool to identify and reduce privacy risks
- Integral part of "Privacy by Design"
- More effective and efficient processes for handling data

When is a PIA required under GDPR?

- Article 35 GDPR provides that a PIA is required in relation to:

a) "systematic and extensive evaluation…which is based on automated processing, including profiling, and which decisions are based that produce legal effects, or similarly significant effects on a person";

b) Large scale processing of sensitive data;

c) Systematic monitoring of a publicly accessible area on a large scale.

Bates Wells Braithwaite

Privacy Impact Assessment (2)

How do you conduct a PIA?

- Article 35(7): the assessment must contain at least:

a) A description of the envisaged processing operations and purposes of the processing, including, where applicable, the legitimate interests of the controller;

b) an assessment of the necessity and proportionality of the processing;

c) an assessment of the risks and the rights and freedoms of data subjects;

d) the measures envisaged to address the risks, including safeguards, and security measures, taking into account the rights of data subjects.

- The DPO (where relevant) should be involved in the assessment.
- See ICO guidance – Conducting PIAs: Code of Practice

Bates Wells Braithwaite

Who needs a data protection officer?

New requirement for DPOs where:

1. Processing is carried out by a **public authority or body** (except courts)

2**. Core activities** involve **regular and systematic monitoring** of individuals **on a large scale**

3**. Core activities** involve processing **sensitive personal data** (or data relating to criminal convictions and offences) **on a large scale**

- If DPO not required, keep a record of that decision

Bates Wells Braithwaite

What is the role of the DPO?

- Advisory role – report to highest management level
- Monitor compliance with GDPR
- Contact point for ICO and data subjects
- Advise on DPIAs
- Expert knowledge of data protection law and practices
- May not be dismissed or penalised for performing tasks
- Must be independent

Bates Wells Braithwaite

Security, breaches and non-compliance

Bates Wells Braithwaite

Security

- “Integrity and confidentiality” principle and Art 32 require appropriate technical and organisational security measures, eg
  - pseudonymisation and encryption
  - disaster recovery
  - testing security measures
- Consider audit, training and policies (including breach response plan)

Bates Wells Braithwaite

Breach notification & communication

- Breach = breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Notification by the controller to ICO:
  - without undue delay
  - where feasible, within 72 hours of awareness
  - unless unlikely to result in a risk to the rights and freedoms of data subjects
- Communication to the data subject where the breach is likely to result in a high risk to the rights and freedoms of data subjects

Bates Wells Braithwaite

Non-compliance

- ICO has range of investigative, corrective, authorisation and advisory powers
- Individuals have rights to bring complaints to ICO and legal action against data controllers and processors
- Certain breaches subject to fines of up to €20,000,000 or 4% of global turnover, whichever is higher (infringement of data protection principles, data subjects' rights, rules on international transfers)
- Maximum fine of €10,000,000 or 2% global turnover for other breaches

Bates Wells Braithwaite

Workshop

Bates Wells Braithwaite

Workshop

Discussion point 1:

- On a scale of 1-5, how ready are you for GDPR? (1=what's GDPR?; 5=ready to go)

Discussion point 2:

- What is your biggest concern:
  a) Resources
  b) Data breaches
  c) Getting my organisation to take it seriously
  d) Data processing contracts
  e) Data subjects' rights
  f) Other?

Bates Wells Braithwaite

Case study

1) You decide to engage an outsourcing company to run a help line for technical queries on your product over the phone. The phone operatives record data from companies and individual users both for marketing purposes and contractual /account matters. **What GDPR issues arise?**

2) An individual employed in a BDIA member's HR team takes a USB stick containing CVs, job applications and equal opportunities forms including requests for reasonable adjustments, out of the office to review at home. The employee loses the USB stick on the way home. **What should the BDIA member do? What if the USB stick had been encrypted?**

Bates Wells Braithwaite

Practical steps

Bates Wells Braithwaite

What should your organisation be doing now?

1. Consider how your organisation is processing personal data and the conditions it is relying on
2. Review privacy notices and policies to ensure they are GDPR compliant
3. Review and update data processing agreements
4. Review and update policies on individual rights – training?
5. Appoint a DPO?
6. Review governance and accountability arrangements – record keeping?
7. Review and update policies on breach reporting – training?

Bates Wells Braithwaite

Questions?

Bates Wells Braithwaite

Contact details

Thank you for attending.

Melanie Carter	m.carter@bwbllp.com	020 7551 7610
Alistair Williams	a.williams@bwbllp.com	020 7551 7743

Bates Wells Braithwaite