The EU General Data Protection Regulation

LawWorks Roundtable

Ceri Chave & Robert Maddox

- Debevoise & Plimpton LLP

Lesley Tadgell-Foster

- National Council for Voluntary Organisations

2 March 2018

Debevoise & Plimpton

Aims & Outcome

- Gain familiarity with key GDPR concepts and obligations
- Give you a basic framework to begin working through towards GDPR compliance
- Improve your GDPR confidence
- Allow you to identify data protection issues and know how to address them

What is data protection?

- Affords individuals the rights to control how their personal information is used
- Places a range of obligations on organisations to process personal data fairly and lawfully
- Central premise behind data protection is balancing individual and business rights through transparency and accountability

What is the GDPR?

- Primary law regulating how companies protect individuals' data
- Comes into force on 25 May 2018
- Regulates those who:
  - process personal data in the EU
  - process personal data of EU-located individuals

- Applies to controllers and processors
  - Controller decides how and why personal data is processed
  - Processor acts on behalf of controller (e.g. local IT professional, third party fundraiser, mailing house)
  - Most clinics will be controllers – they collect, store and/or process personal data
- Increased penalties for breach

Why does it matter to clinics?

- GDPR applies to everyone – from clinics to large multinational corporations
- Handle personal data – beneficiaries, donors, trustees, volunteers, employees
- Deal with vulnerable people – mental health, physical health; children
  - Higher risk = greater protection
- Legal risk
  - Fines of up to 2% or 4% of total global annual turnover or EUR 10m or EUR 20m, whichever is greater
- Reputational impact
  - Loss of trust

Enforcement Action Against Charities

- Fined £18,000 and £25,000
- Secretly screened millions of their donors ("wealth screening")
- Traced and targeted donors by piecing together personal information obtained from other sources
- Traded personal details with other charities
- "*The law exists to protect people's rights and it applies irrespective of how altruistic the organisation's motives might otherwise be*"
  - Elizabeth Denham, Information Commissioner

Enforcement Action Against Charities

CANCER RESEARCH UK

NSPCC

OXFAM

Myth Busting – Fines

The Myth

- The biggest threat to organisations from the GDPR is massive fines
- Fines will be bigger than under the Data Protection Act

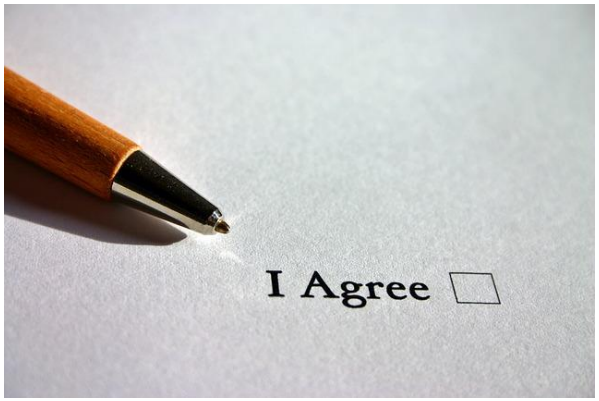
The Reality

- The maximum fines are increasing
- The ICO has never used its current maximum fine
- ICO is committed to guiding, advising and educating organisations about how to comply with GDPR
- "*We have always preferred the carrot to the stick*"
  - ICO, 9 August 2017
- Fines are the ICO's last resort
- Of 17,300 cases in 2016/17 there were only 16 fines

Myth Busting – Consent

The Myth

- You must have consent to process personal data



The Reality

- The GDPR raises the bar for valid consent
- But consent has always required clear affirmative action
- Consent is one way to comply with GDPR but it is not the only way
- "Consent is not the 'silver bullet' for GDPR compliance"
  - *ICO, 16 August 2017*
- In many cases, consent will not be appropriate

Myth Busting – The GDPR Burden

The Myth

- GDPR is an unnecessary burden on organisations

The Reality

- Many fundamentals remain the same
- Evolution not a total revolution
- Many of the GDPR's requirements scale to risk
- "Whatever the size of your organisation, GDPR is essentially about trust"
  - *ICO, 25 August 2017*

Myth Busting – Breach Reporting

The Myth

- All personal data breaches have to be reported to the ICO and affected individuals
- All details have to be provided immediately
- If you don't report, you will be fined

The Reality

- ICO – You only have to report if it's *likely* to result in a risk to people's rights and freedoms
- Individuals – You only have to notify if there's the likelihood of a *high* risk to people's rights and freedoms
- High risk situations likely to include potential discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage
- Information can be given when available
- Failure to report will not always result in a fine

Debevoise & Plimpton

What is personal data?

- Any information that can directly or indirectly identify a natural person – very broadly defined and includes:
  - Name, age, date of birth, address, photo
  - Email and IP addresses, location data
  - Publicly available information
  - Two or more non-specific pieces of information that could identify an individual (e.g. combining gender and birth date)
- Sensitive personal data:
  - Racial/ethnic origin data
  - Religious beliefs
  - Health data (including physical or mental health or condition)
  - Genetic data
  - Children

What should I do first?

- Audit the personal data you hold about beneficiaries, donors, volunteers and staff:
  - What personal data do you hold?
  - Where did it come from?
  - What do you do with it and what do you plan to do with it?
  - Have you documented your findings?
  - Do you keep records of your processing activities?
  - Do you share any data with third parties?
  - Do you keep a record of data shared with third parties?
- This will also help inform your privacy notice

What are the key principles?

6 key principles:

- **Lawfulness, fairness and transparency** - i.e. you have to process personal data in a lawful, fair and transparent manner
- **Purpose limitation** – use for specified reasons only
- **Data minimisation** – only collect the data you need
- **Accuracy** – erase or rectify out of date/inaccurate data
- **Storage limitation** – only keep data as long as necessary; depersonalise if keeping it for analysis
- **Integrity and confidentiality** – protection against unauthorised processing and accidental loss
- **Accountability** – clinic is responsible for, and must *demonstrate* compliance with GDPR
    - E.g. record-keeping, documentation, policies, procedures and audits

When can you process personal data?

- You must identify and document the lawful basis for all processing of personal data, and update your privacy policy:
  - Direct consent from the individual (e.g. actively ticking the “yes” box on donation form to processing personal data)
  - Necessary for the performance of a contract (e.g. third parties that process data on your behalf, such as external payroll providers)
  - Compliance with a EU or MS legal obligation (e.g., EU AML laws)
  - Legitimate interest pursued by the clinic (e.g. processing for direct marketing purposes; reporting potential criminal acts)
  - Protecting the vital interests of the individual (e.g. life-or-death scenarios)
  - Necessity for the public interest (i.e. are you carrying out a task in the public interest or exercising official authority)

What is valid consent?

- Heightened consent requirements
- Freely given, specific, informed and unambiguous, statement or affirmative action
  - **Unbundled** - separate from general terms and conditions
  - **Active opt-in** - no pre-ticked boxes
  - **Named** - clear who is given consent; not just 'third parties'
  - **Documented** - records are kept of the consent)
  - **Easy to withdraw** - should be able to withdraw the same way given
- Revisit and refresh consents?
- Mailing lists – do you have valid consent?
- Record keeping is key

What do we have to tell service users?

- Tell people what you are doing with their data!

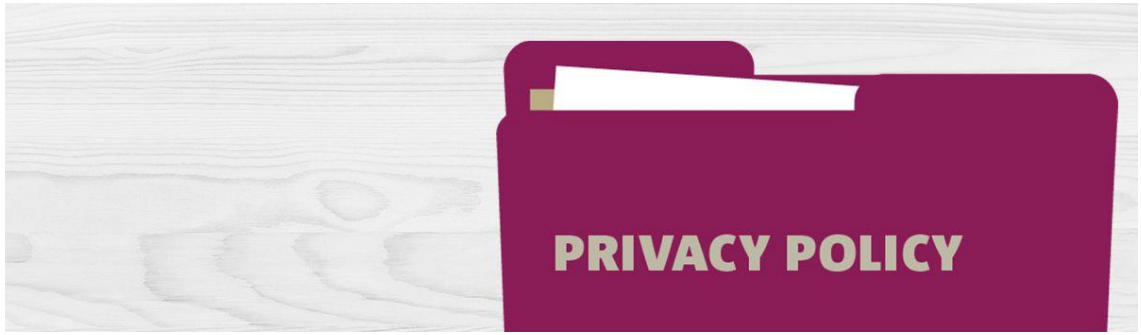
- Identity and contact details of the clinic (i.e. the data controller)
- The purposes of the personal data handling and legal bases for that handling (e.g. consent/legitimate interests)
- Recipients or categories of recipients of the personal data
- Details of data transfers outside of the EU
- Length of time for which the personal data will be stored and/or the criteria used to determine that period
- How the organisation ensures data is kept accurate and when data will be deleted
- Under what circumstances the clinic discloses data and to whom
- How the clinic keeps individuals informed about the data it holds
- Who is responsible for reporting any breaches to the ICO and the Charity Commission
- The right to correct inaccurate personal data or, in certain cases, to have personal data erased
- The right to move personal data from one service provider to the other
- What to do if an individual asks to see their data and when you will turn down a Subject Access Request
- How data should be stored and backed up
- The right to object to processing of personal data
- An individual's right to complain to a supervisory authority about the handling of their personal data

What rights do people have and how should you prepare?

- Right to be informed of how personal data is processed
- Right to request correction or erasure of personal information
- Right to restrict and object to processing in certain circumstances
- Right to not be subject to automated decision making
- Company must respond to requests without undue delay and within one month of receipt

What do we have to tell service users?

- Suggestions for how your privacy notice can be communicated:
  - When a user comes to the clinic, provide them with a privacy notice
  - Ask them to read it and sign it
  - Keep a record of the users who have signed the privacy notice
  - Store all signed privacy notices
  - Destroy when no longer necessary



What should we tell volunteers/employees?

- Volunteers and employees have GDPR rights
  - Update privacy notices given to volunteers/employees to ensure GDPR compliant
  - Update employment contracts to reflect GDPR
- Volunteers and employees have obligations
  - Provide periodic training – GDPR is a shared responsibility
  - Instil good practices amongst volunteers/employees – "Think GDPR"
- Monitor compliance with data protection-related safeguards and reward people for compliance

How should we store records?

- Obligation to safeguard data
- Technology can help:
  - Strong passwords
  - Encrypted USB drives
  - Password protected files
  - Restricted access
- Don't forget the low tech:
  - Locked filing cabinets?
  - Who has the keys to the building?
  - Clear desk policy?
  - Records of hard copy files?

How long should we keep records for?

- Obligation to only keep data so long as is necessary
- Will not be the same for all types of personal data
- Think about what personal data you have, why you have it, and what you told the individual about how long you would have it
- Examples:
  - Mrs. A storms out after 30 seconds of the appointment
  - Mr. B helped to resolve his issue successfully
  - Mrs. C very unhappy with outcome of her issue and threatens to sue
  - Volunteer D has moved to Australia
- Document the approach you are going to take
- Revisit the data you hold periodically (look back now…)

What should we do if there is a data breach?

- New obligation to report a "personal data breach", subject to materiality threshold, to ICO

- Personal data breaches can include:
  - access by an unauthorised third party;
  - sending personal data to the wrong person;
  - devices containing personal data being lost or stolen;
  - alteration of personal data without permission; and
  - loss of availability of personal data

What should we do if there is a data breach?

- ICO:
  - What: breaches likely to pose a "risk to [individuals'] rights and freedoms"
  - When: within 72 hours, unless risk to individuals is unlikely
- Affected individuals:
  - What: breaches likely to pose "a high risk to the [individuals'] rights and freedoms" e.g., identity theft, potential discrimination, damage to reputation, financial loss
  - When: without undue delay

What should we do if there is a data breach?

- Report it online or via telephone
  - https://ico.org.uk/for-organisations/report-a-breach/
- What does the notification need to include?
  - What?
  - When?
  - How found out?
  - Who (potentially) affected?
  - What are you doing about it?
  - Who should the ICO contact?
- Contact individuals as best you can

What should we do if there is a data breach?

- What does the ICO say you should be doing to prepare?

Preparing for a personal data breach

☐ We know how to recognise a personal data breach.

☐ We understand that a personal data breach isn't only about loss or theft of personal data.

☐ We have prepared a response plan for addressing any personal data breaches that occur.

☐ We have allocated responsibility for managing breaches to a dedicated person or team.

☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

What should we do if there is a data breach?

- How does the ICO say you should respond to a breach?

Responding to a personal data breach

☐ We have in place a process to assess the likely risk to individuals as a result of a breach.

☐ We know who is the relevant supervisory authority for our processing activities.

☐ We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

☐ We know what information we must give the ICO about a breach.

☐ We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.

☐ We know we must inform affected individuals without undue delay.

☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.

☐ We document all breaches, even if they don't all need to be reported.

Data Breach – A Worked Example

- Service User A has been fired from work
- Thinks it was due to medical condition
- Volunteer records details of health condition in hardcopy file
- Puts hardcopy file in bag by mistake
- Bag left on train and not recovered

Data Breach – A Worked Example

- Service User B has been fired from work
- Thinks it was due to medical condition
- Volunteer records details of health condition in digital file
- Saves to encrypted USB drive
- Bag left on train and not recovered

Beware of Personal Liability

- Rochdale Connections Trust charity worker sent spreadsheets containing vulnerable clients' information to his personal email
- 11 emails containing sensitive personal data relating to 183 people including 3 children
- Admitted to unlawfully obtaining personal data at Preston Crown Court
- Two year conditional discharge, costs of £1,845.25 and £15 victim surcharge

"People whose jobs give them access to this type of information need to realise that just because they can access it, that doesn't mean they should"

- Steve Eckersley, Head of Enforcement, ICO

Useful Resources

- ICO Website:
  - https://ico.org.uk/for-organisations/charity/charities-faqs/
- Fundraising Regulator:
  - https://www.fundraisingregulator.org.uk/faqs/charity-faqs/
- The GDPR:
  - http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
  - https://gdpr-info.eu/

"GDPR compliance will be an ongoing journey"
- ICO, 22 December 2017