Mersey Internal Audit Agency

The new General Data Protection Regulation (GDPR)

Suzanne Crutchley LLM
Senior Information Governance Associate
Mersey Internal Audit Agency

6th October 2017

CELEBRATING 25 YEARS OF MIAA

Will you be ready in time?

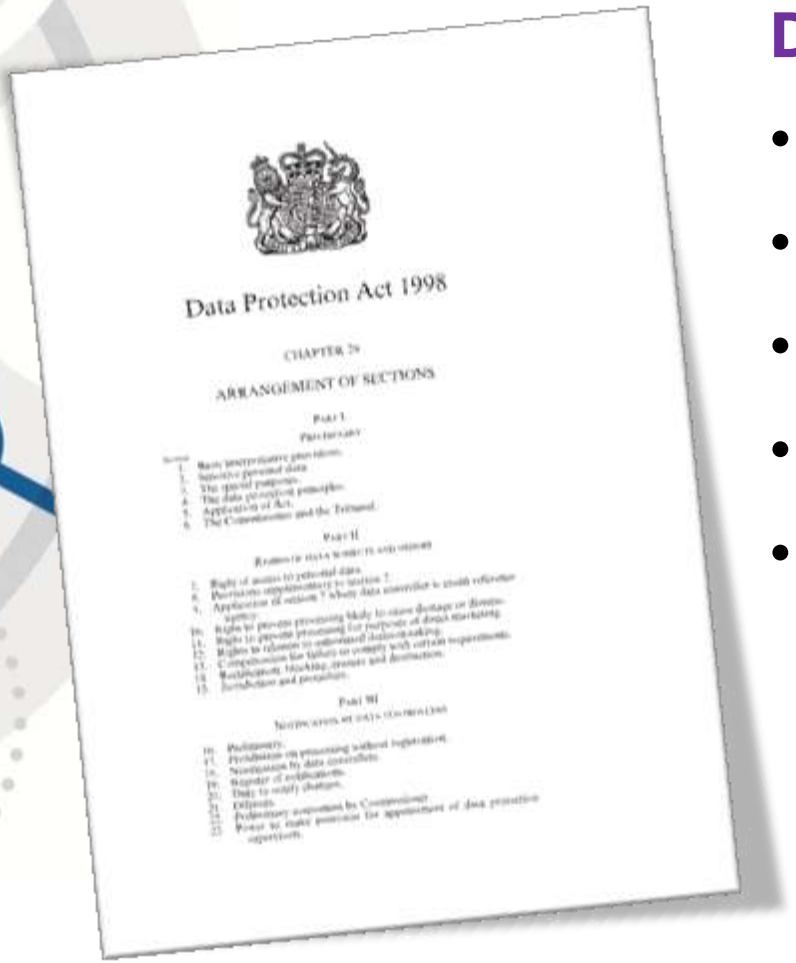
- *Is your organisation **sufficiently resourced** with staff and skills to discharge your obligations under the GDPR?*

- *Even if you are compliant with the Data Protection Act, this will not be sufficient to be **GDPR compliant**.*

GDPR Introduction

- **Four years** in the making.
- Final text published **May 2016.**
- Enforced on **25th May 2018**, after a two-year transition.
- **Replaces** the national laws and regulations based on the 1995 EU Data Protection **Directive 95/46/EC.**
- As a regulation, the GDPR will have **direct legal effect** throughout the EU, without requiring transposition into national legislation.

Current data protection law in the UK and EU


Data Protection Act 1998

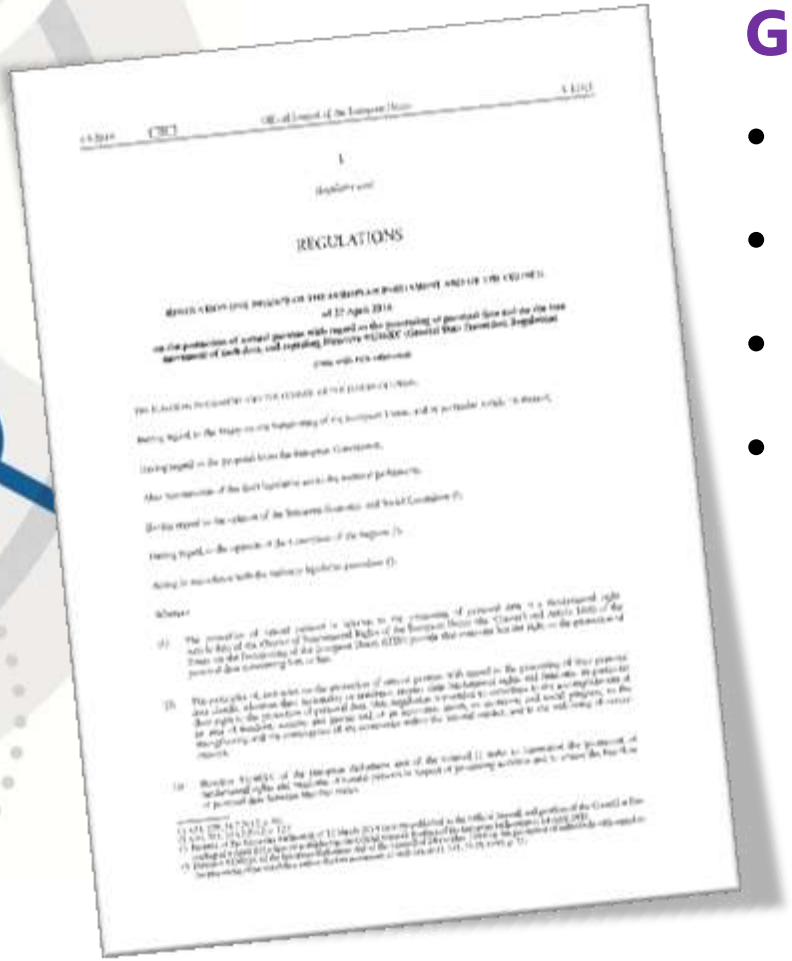
CHAPTER 29

ARRANGEMENT OF SECTIONS

Data Protection Act 1998

- In force since 2000
- 92 pages
- 75 Sections
- 8 Schedules
- Almost 100 ICO guidance documents

Future data protection law in the UK and EU


REGULATIONS

General Data Protection Regulation

- Comes into force on 25th May 2018
- 88 pages
- 173 recitals
- 99 articles

Why change?

- To update the law to better address **contemporary privacy challenges**, such as those posed by the Internet, social media, mobile apps, cloud computing, "big data," and behavioral marketing, that were in their infancy when the Data Protection Directive was drafted.
- GDPR raises the bar to provide **better privacy protection for individuals**.

Organisations should be looking ahead to the new compliance landscape in their product design, operational planning, privacy policies, security systems, and contracts, beginning …

…well, now!

Article 5 – Six Principles

- Fair and lawful and transparent processing.
- Obtained only for specified, explicit, legitimate and lawful purposes and not processed in an incompatible manner.
- Adequate, relevant and not excessive.
- Accurate and up to date – every reasonable step taken to ensure inaccurate personal data is erased or rectified without delay.
- Not kept longer than necessary.
- ~~Processed in accordance with data subject rights.~~
- ~~Protected by appropriate technical and organisational measures.~~ Processed in a manner that ensures appropriate security.
- ~~Not transferred outside of the EEA unless adequate protection is in place.~~
- The controller is responsible, and able to demonstrate compliance.

Brexit means Brexit… or does it?

- The GDPR will come into force before Brexit.
- **Article 3 – territorial scope** - GDPR applies to:
  - Processing of personal data in relation to activities of an EU controller/processor.
  - Processing of personal data of EU data subjects, in relation to the offering of goods or services, or monitoring of their behaviour within the EU, by a non-EU controller processor.

Data Protection Bill

Government introduces Data Protection Bill in House of Lords

- The **Data Protection Bill** was introduced into the House of Lords on 13th September 2017.
- It will replace the Data Protection Act 1998 and implement the EU General Data Protection Regulation (GDPR).
- The Bill differs from the GDPR in that it also covers, in addition to processing of personal data to which the GDPR applies, law enforcement data and national security data.

Accountability and Governance

- These provisions complement the GDPR's **transparency requirements**. Whilst previously implicit under DPA, the GDPR's emphasis elevates their significance.
- You are expected to put into place **comprehensive** but **proportionate** governance **measures**.
- Ultimately, these measures should **minimise** the risk of **breaches** and **uphold** the **protection** of personal data.
- Practically, this is likely to mean **more policies and procedures** for organisations, although many organisations will already have good governance measures in place already.

Individuals' rights

The GDPR provides the following **rights for individuals**:

- ✓The right to be informed
- ✓The right of access
- ✓The right to rectification
- ✓The right to erasure
- ✓The right to restrict processing
- ✓The right to data portability
- ✓The right to object
- ✓Rights in relation to automated decision making & profiling

Enforcement

- Like the Directive, the Regulation contemplates enforcement both through the **supervisory authorities** and the **courts**, with penal and administrative sanctions as well as civil remedies.

- But the Regulation ups the ante for **administrative penalties**, which can be as high as **€10 million or 2% of your turnover, or double this in some cases!**

How can I demonstrate that I comply?

- Maintain documentation on **processing activities**.
- Appoint a **Data Protection Officer**.
- Implement measures that meet the principles of **data protection by design** and **data protection by default**.
- Conduct **data protection impact assessments** where appropriate.
- Adhere to approved **codes of conduct** and/or **certification** schemes.

Security

- The current Directive required appropriate **technical and organizational measures t**o safeguard personal data.
- The new Regulation goes beyond this, not only by requiring notice and documentation of **security breaches**, but also referring to a **risk evaluation** and the Commission's authority to **adopt specific security requirements.**
- Consider conforming to **internationally accepted security management standards** (**ISO 27001/27002**), as these are more readily understood in Europe and will likely be referenced in the Commission's implementing measures.

Privacy Governance and Documentation

- GDPR obliges controllers, processors, and representatives to maintain **documentation** of specified aspects of **personal information handling**, and to make it available on request.
- Data controllers will be responsible for **designing & implementing mechanisms to protect** personal data and ensuring that, **by default**, personal data are:
  - **collected** and **used** only as necessary for specific purpose(s)
  - **retained** no longer than necessary
  - not made **available** to an indefinite number of persons

Privacy Policies and Communications

- Where the controller uses **automated means**, it must **provide for** data subjects to submit **choices, requests, and complaints** electronically.

- If the controller makes requested **corrections or deletions**, it must also communicate those to any **third-party recipients** of the data, if feasible.

Stricter Conditions for Consent

- The data controller bears the **burden of proof** for establishing **consent**, which means that some form of writing, click-through, or other procedure typically must be in place as evidence.

(N.B. silence, pre-ticked boxes or inactivity does not constitute consent.)

- The data subject must have the **right to withdraw consent** at any time for future processing.

The problem with patient consent

- Currently, flows of information for the purposes of direct care of patients is on the basis of consent – including *implied consent* (as per Caldicott reviews).
- **However, under GDPR:**
  - Consent cannot be implied.
  - Consent can be withdrawn.
  - Processing on the grounds of consent gives rise to additional rights.
- Therefore, the NHS should not rely on consent for purposes of GDPR, and rely on *provision of health or social care* instead - **Article 9 2. (h).**

Article 17 – right to erasure

"Right to be forgotten"

- Data controllers must erase on request where:
  - Personal data no longer necessary for purposes.
  - Data subject withdraws consent.
  - Data subject objects to processing.
  - Unlawful processing.
- Does not apply if processing is necessary:
  - Tasks carried out in public interest / in exercise of official authority.
  - Protection of public health.
  - Establishment, exercise or defence of legal claims.

Article 19 – right to data portability

- Right to receive personal data in a structured, commonly used and machine-readable format and able to transmit, without hindrance, to a new controller.
- Only applies if:
  - Processing based on consent or pursuant to contract; AND
  - Carried out by automated means.
- Another reason not to rely on consent!

Sensitive Data

- ***Special categories*** of especially sensitive data require express consent or a legal obligation in order to collect or process the data, and they require **heightened security** and attention to **data storage limits**.

- The Regulation adds **genetic** and **biometric** data to the **categories** of sensitive data.

- If you offer an 'information society service' (i.e. target online services) at **children**, you will need to obtain **consent from a parent or guardian** to process the child's data.

Direct Marketing and Profiling

- These provisions include the "**Right to object**" and "**Measures based on profiling**" e.g. transactions based on risk scores.

- Identify whether any of your processing operations constitute **automated decision making** and consider whether you need to update your procedures to deal with the requirements of the GDPR.

Data Breach Notice and Documentation

- The Regulation requires **notice of any personal data breach** to the **supervisory authority within 24 hours**, followed by **notice to the individuals** of personal data breaches *"likely to adversely affect the personal data or privacy of the data subject,"* unless the controller satisfies the authority that the data were rendered unintelligible (such as by encryption).

- The Regulation also requires fairly **extensive documentation** of security incidents.

International Data Transfers

- GDPR imposes restrictions on the transfer of personal data **outside the European Union,** to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.
- The Regulation preserves the **legal mechanisms** accepted under the Directive for transferring personal data outside the EU/EEA.

Data Protection Officer

- Must appoint a **Data Protection Officer** (DPO) if you employs 250 or more persons or if your core activities require *"regular and systematic monitoring of data subjects"*.

- Must ensure DPO reports to the highest management level of your organisation – i.e. **Board level**, and that there are adequate resources provided to enable DPOs to meet their GDPR obligations.

- DPO position needs to be independent of other key positions, so that there is **no conflict of interests**.

DPO Role

- DPO informs/advises organisation, monitors compliance, and acts as point of contact for ICO.
- May be one DPO for a number of organisations.
- Must have expert knowledge of data protection law and practices.
- Must be properly involved in all DP issues.
- **Must be able to act independently** – supported, and not discriminated against by management.
- Could Caldicott Guardian / SIRO be DPO? Could that lead to a conflict of interests?

Guidance and Derogations

- **ICO** has published some guidance and will continue to do so.
- **Information Governance Alliance** will roll out NHS-specific guidance on a series of topics.
- Government is consulting on derogations.
- Things should become clearer over the next few months, but time is already very limited.

Governance, Regulation and Enforcement

- Public bodies must have a Data Protection Officer.
- Prior consultation with ICO for high risk processing.
- Mandatory breach notification without delay and within 72 hours, unless unlikely to present risk to data subjects.
- Notification to data subjects where breach is high risk.
- Compensation for material and non-material damage (e.g. distress).
- Maximum fine increased from £500k to **€20m.**

What to Do Now?

- Might sound a long way off, but there is **much to do** for the many organisations that will need to be in compliance **by 25th May 2018**.
- As we edge ever closer to the official launch of GDPR, there will be **two types of organisations:**
  - those that will only start making changes once GDPR comes into force;
  - those who are prepared for GDPR in advance.

The latter, of course, have the upper hand.

Getting ready for the GDPR

- **People:**
  - Your Chief Executive/Officer needs to know about GDPR.
  - Appoint DPO – to meet GDPR requirements.
  - Who else is responsible - working group.
  - Board training.
  - Staff training.
- **Support:**
  - ICO and IGA Guidance
  - Advice
  - Audit

Stocktake for GDPR

Stocktake: identify, review and update…

- Information Asset Register (IAR).
- Data Flow Mapping (DFM).
  - Review legal conditions for data processing.
  - Establish records of all processing activities.
- Relevant Policies – & create new ones for new rights/obligations – e.g. right to erasure, breach reporting, Subject Access Requests (SARs), etc.
- Data Processing Agreements – especially involving international transfers.
- Privacy notices.
- Retention periods.
- Systems – accountability and data protection by design
- Use new Data Protection Impact Assessments (DPIAs).
- Security measures.

State of readiness

- Mersey Internal Audit Agency can provide an **independent audit** of where your organisation is currently in data protection terms, and what you need to do ahead of the 25th May 2018 implementation date for the new GDPR.
- This audit will look at all your **current data protection arrangements**, and will specifically cover all the areas above.
- We will **meet with a range key individuals** within your organisation, including relevant directors, managers and operational staff, and using our **diagnostic tool** we will identify the current organisational position, across key themes.
- Our resulting **reporting** and action plan will highlight the **key developments and actions** that are required by the organisation to ensure compliance with GDPR by the time of its introduction.

Independent Audit

- ✓ To discuss how MIAA can work with you to deliver this assessment within your organisation please contact:

Tony Cobain

Assistant Director – Informatics & Infrastructure

Mersey Internal Audit Agency

Tel: 07770 971006

tony.cobain@miaa.nhs.uk

Thank you