The General Data Protection Regulation (GDPR)

Leyla Hannbeck MRPharmS, MBA, MSc, MA

NPA Chief Pharmacist and Director of Pharmacy

Data protection law: what is changing?

Data Protection Directive → **General Data Protection Regulation (GDPR)**

(Applies from 25 May 2018)

+

Data Protection Act 1998 (DPA) → **Updated Data Protection Act**

(The Data Protection Bill is currently passing through UK parliament)

Brief overview of the GDPR

Effective date: 25 May 2018

GDPR: brief overview

- **GDPR is being brought to the attention of the general public**
- Many concepts and principles similar to existing DPA
- **New elements** and **significantly enhanced requirements**
- Key changes include:
  - Updated data protection principles and scope
  - Updated conditions for processing data
  - New rules regarding consent
  - Enhanced data subject rights
  - New, specific legal responsibilities for organisations processing children's data
  - New obligations for data controllers and processors
  - New addition of **the '*accountability principle*'** and the role of the '*Data Protection Officer*"
  - Greater regulation and enforcement

Public awareness via media!!!!

Data Protection Act	The General Data Protection Regulation
Only applicable in UK	Applies to all EU countries
No requirement for a data protection officer (DPO)	Appointment of a data protection officer (DPO) required for certain organisations
Consent: does not necessarily require positive opt-in	Consent: must be specific, positively opted-in and not implied
Covers personal data and sensitive personal data	Covers personal data and special categories of data (which includes genetic/biometric data, location data and online identifiers)
Responsibility lies predominantly with the data controller	Responsibility lies with both the data controller and processor
Comparably less accountability	Accountability principle explicitly defined
Subject access request: £10 and within 40 days	Subject access request: free of charge and within 30 days

GDPR: application

GDPR applies to:	Exemptions to GDPR:
All data controllers and data processors • A **data controller** determines how and why personal data is processed • A **data processor** carries out the processing on behalf of the data controller	Certain activities are exempt from GDPR requirements including those: • Covered by the Law Enforcement Directive • Used for national security purposes • Carried out by individuals purely for personal/household activities

GDPR: personal data

- Personal data includes:
  - Information manually held in filing systems
  - Automated personal data
  - IP address
- '*Special categories of personal data*'
  - Similar to the concept of sensitive personal data under the current DPA
  - GDPR includes genetic/biometric data where it is processed to identify an individual

GDPR principles and accountability

GDPR: data protection principles

The **six data protection principles** identified under the GDPR state that personal data **must be**:

1. *Processed lawfully, fairly and transparently*
2. *Collected for specified, explicit and legitimate purposes*
3. *Adequate, relevant and limited to what is necessary in relation to the purposes of processing*
4. *Accurate and where necessary, kept up to date*
5. *Kept in a form which allows the identification of a data subject for no longer than is necessary*
6. *Processed in a manner that ensures appropriate security*

GDPR: accountability principle

- Aim: to **minimise risk** of data breaches and promote protection of personal data
- Organisations are required to implement comprehensive **governance** measures, which must be proportionate to their processing
- It is the organisation's responsibility to ensure they are able to **demonstrate compliance**

GDPR: demonstrating compliance

- **Implement** appropriate technical and organisational measures
- Maintain **relevant documentation** on processing activities
- Appoint a **Data Protection Officer** (DPO)
- Use **data protection impact assessments** (where appropriate)

GDPR: data protection officer (DPO)

- Under the GDPR, a DPO is required if an organisation carries out '***large scale processing of special categories of data***'
- **No training** is required for the role of a DPO however, the DPO is expected to have adequate knowledge of data protection law
- ICO have stated that the DPO can be an **existing employee** of an organisation
  - Professional duties should be compatible with DPO duties and there must be no conflicts of interests

Relevant records and documents

- Records of **processing**
- **Privacy notice**
- Records of **consent**
- **Location** of personal data within the organisation
- **Contracts** between controllers and processors (where applicable)
- Records of **data breaches**

Lawful basis for processing

GDPR: Lawful basis for processing

1. Data subject provides **consent** to the processing of their personal data for one/more specific purposes
2. Data processing is necessary due to a **contract** in place or prior to an individual entering into a contract
3. Data processing is necessary for compliance with a **legal obligation** to which the controller is subject
4. Data processing is necessary to **protect** the vital interests of the data subject /another natural person
5. Data processing is necessary for the **performance of a task** undertaken in public interest or to exercise of official authority vested in the controller
6. Data processing is necessary for the **controller/third party legitimate interests**; except where the data subject's rights and freedoms overrides it, particular if the data subject is a child – this does not apply to data processing by public authorities in the performance of their tasks

GDPR: Lawful basis for processing

- **Dispensing a prescription**
  - A patient effectively implies consent to enable the pharmacy to process their personal data for the purpose of dispensing a prescription
  - Lawful basis: *processing is necessary for the* ***performance of a task carried out in the public interest or in the exercise of official authority vested in the controller***
- **Deliveries of dispensed items**
  - This service does not fall under the pharmacy contract consent is required to enable a pharmacy to use an individuals personal data for the purposes of a delivery
  - Lawful basis: *the data subject has given* ***consent to the processing of his or her personal data for one or more specific purposes***

GDPR: consent

Must be	Cannot be
Given freely, be specific, informed and unambiguous	Assumed from the individual's lack of action/response
Obtained by clear affirmative action	Through pre-ticked consent boxes
Verifiable and positively opted-in	Obtained by default or by using opt-out boxes
Simple/straightforward to withdraw consent	Part of any terms and conditions of a service

Consent:

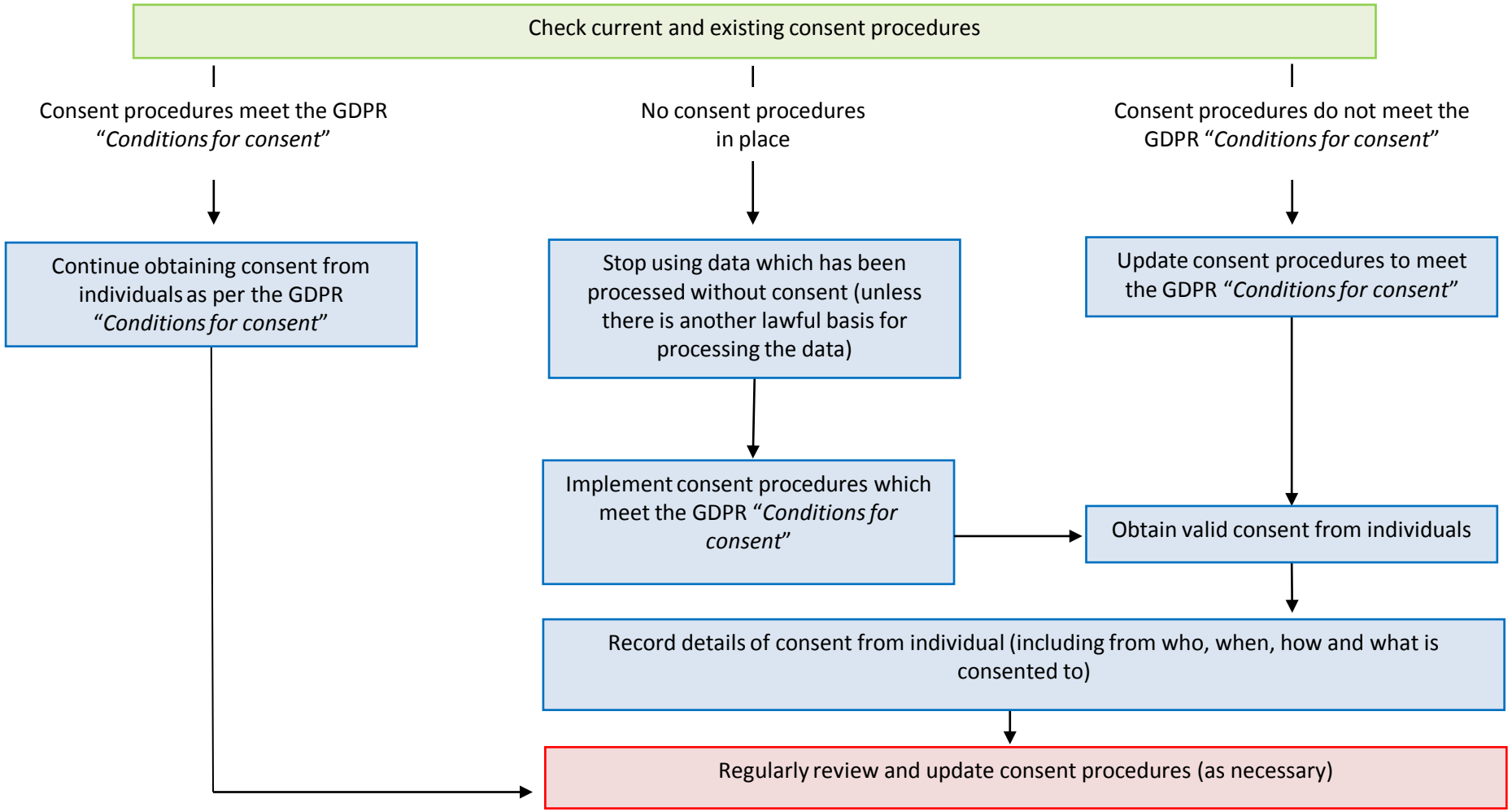
- May not always be required – remember there are five other lawful bases permitting the processing of an individual's personal data
- Must be obtained where another lawful basis for data processing is not applicable

GDPR: consent

The Information Commissioner's Office (ICO) recommendations:

- Regularly review and update consent and associated procedures (as necessary)
  - There is **no** set time limit/expiry date for consent validity
- Keep records of evidence
  - Including the name of individual providing consent, how consent was provided and date/purpose for consent

GDPR: consent



Individual rights

GDPR: individual rights

- The rights of individuals under the GDPR are **similar** to those under the DPA; however, there are notable **enhancements**
- The GDPR provides **eight rights** for individuals
- Not all of the rights are absolute – some rights are only applicable in **certain circumstances**

GDPR: individual rights

1. The right to be **informed**
2. The right of **access**
3. The right to **rectification**
4. The right to **erasure**
5. The right to **restrict processing**
6. The right to **data portability**
7. The right to **object**
8. Rights in relation to **automated** decision making including profiling

Individual rights: right to be informed

- Organisations must provide **"fair processing information"**
- Fair processing information is usually presented in the form of a **privacy notice**
- Privacy notice must be concise, **transparent**, **intelligible**, and use **clear** and **plain** language

Individual rights: right to be informed

How the individual's personal data is obtained	Time frame for informing the individual of the organisation's *"fair processing information"*
Personal data obtained **directly** from the individual	**At the time** the personal data is obtained
Personal data obtained **indirectly** from the individual	Within a reasonable time frame after obtaining personal data; this should be within **one month**
Personal data obtained **indirectly** from the individual **and** the personal data is used to communicate with the individual	When the **first** communication occurs
Personal data obtained **indirectly** from the individual **and** the personal data is envisaged to be disclosed to another recipient	**Before** the personal data is disclosed to the other recipient (at the latest)

Individual rights: right of access

- Often termed a "**subject access request**"
- The organisation must **verify identity** of the person making the request
- Individuals have the right to:
  1. **Access** their personal data
  2. **Confirm** that their personal data is being processed
  3. **Obtain** other supplementary information

Individual rights: right to rectification

- An individual is able to request rectification if personal data is:
  1. **Inaccurate**
  2. **Incomplete**

- Third party **notification** is required (in certain circumstances)

Individual rights: right to erasure

- Often termed the "**right to be forgotten**" – permits an individual to request **deletion** of their personal data
- Individuals **do not have absolute right** – only applicable in certain circumstances including:
  - The personal data is no longer necessary for the purposes for which it was collected or processed
  - The individual withdraws consent for the lawful processing of their personal data **and** there is no other lawful basis for processing
  - The individual objects to the processing of their personal data **and** there is no overriding legitimate interest to continue processing
  - The personal data was unlawfully processed
  - The personal data must be erased to comply with a legal obligation

Individual rights: right to erasure

A request to erase an individual's personal data can be rejected by an organisation, if at least one of the following applies :

- When exercising the right of **freedom of expression and information**
- Complying with a **legal obligation** for the performance of a public interest task or exercise of official authority
- If in the **public's interest**, for public health purposes where "*processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care treatment or the management of health or social care systems and services*"
- If the data is required for **archiving purposes** which is in the interest of the public, for historic/scientific research, or statistical purposes
- Establishment, exercise or defence of **legal claims**

GDPR: complying with an individual's request to exercise their right

- Take reasonable steps to **verify the identity** of the individual
- Comply without undue delay and within **specified time frames (one month)**
  - Time frames differ for the '*right to be informed*'
- Organisations must provide the information **electronically**, where possible
- Provide the information **free of charge**

Data breaches and implications

GDPR: data breaches

- A personal data breach means a **breach of security leading to the destruction**, **loss**, **alteration**, **unauthorised disclosure of**, or **access** to **personal data**
- Requirement for organisations to **report** certain types of **data breaches** to the ICO
  - Breaches must be **reported** within **72 hours**
  - **Failure to report can result in a fine** of up to **€10million or 2 per cent** of the organisation's global turnover
- In some cases, the organisation must contact the **affected individual(s)**

GDPR: data breaches

- A personal data breach includes:
  - **Loss/theft** of personal data
  - **Sending** personal data (such as medicines with patient name/address) to an incorrect recipient
  - **Altering** patient information without consent
  - **Unauthorised** individuals accessing patient information from a PMR

- An affected individual **does not** need to be informed if:
  - Appropriate organisational and technical **protection measures** have been applied
  - **The breach is not highly likely to risk an individual's freedom and rights**
  - Notification would involve **disproportionate effort**

GDPR: implications

- Organisations are obliged to demonstrate **compliance** – the *"accountability principle"*
- Healthcare sector (incorporating community pharmacy) is at **high risk** due to the day-to-day processing of *"special categories of personal data"*
- **Fines** can be imposed on organisations who are in breach of GDPR

How to prepare and NPA support

GDPR: how to prepare

- **Raise awareness** within your organisation of the forthcoming changes, especially with key decision makers
- Ensure individuals familiarise themselves with, and are aware of, the **six lawful bases for processing personal data** under the GDPR
- **Identify** your organisation's lawful basis for processing personal data
- Look into appointment of a **DPO**

GDPR: how to prepare *(cont.)*

- **Consent**
  - Check **current and existing procedures** for obtaining/updating consent in the organisation – this includes how consent is sought, recorded and managed
  - Consider the **services offered** which require consent to process data
    - Services include providing a prescription delivery service or a repeat prescription management service, sending emails/text messages, nominating patients for the Electronic Prescription Service (EPS) and accessing Summary Care Records (SCR)
  - Be aware that inappropriate or invalid consent is **not** a lawful basis for processing personal data

GDPR: how to prepare *(cont.)*

- **Individual rights**
  - Ensure individuals familiarise themselves with, and are aware of the **eight rights of individuals**
  - Be aware of the **time frames** the organisation needs to comply with an individual's request to exercise their right(s)
  - Review and update the **privacy notice**
- **Data breaches**
  - Review and update, if required, your organisation's procedure on managing **data breaches** to comply with the GDPR

GDPR: how to prepare *(cont.)*

- **Data breaches**
  - Check **areas** where a data breach may occur
  - **Familiarise**, be **aware** of, and **recognise** what is considered to be a personal data breach
  - **Allocate** an individual the **responsibility** of managing breaches
  - Ensure a robust system is in place for **detecting and investigating** breaches
  - Be aware when a breach needs to be **reported**
  - **Document** all data breaches within the organisation

GDPR: how to prepare *(cont.)*

- **Relevant records and documents**
  - Perform an **audit** or **data-mapping exercise** in the pharmacy to identify data processing procedures
  - Begin to **review** agreements, contracts, policies and procedures on data sharing, retention and security – both **within the pharmacy** and with **external organisations**
  - Ensure the pharmacy has the required **up-to-date** written **records/documentation** in place

GDPR: NPA support

Current NPA support resources available to members

- Brief overview of GDPR
- Consent – brief overview
- Individual rights – brief overview

Future NPA resources

- Data breaches – brief overview
- Records of processing activities – brief overview
- Lawful basis of processing – brief overview
- Training manual for support staff

NPA Pharmacy team

- NPA members can contact the Pharmacy team on 01727 891 800 for further information and guidance

GDPR: Areas requiring clarification

Previously indentified areas requiring clarification:

- **Sector-specific guidance**
- **Information Governance Alliance (IGA)**
- **Data Protection Bill**
- **IG Toolkit**