GDPR

Data Protection Officer

Leyla Hannbeck
MRPharmS, MBA, MSc, MA

NPA Chief Pharmacist and Director of Pharmacy
Effective date: 25 May 2018

6 - principles of data protection
6 - lawful bases for processing data
8 - individual rights
(668)

Health data = *Special categories of personal data*
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: 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: 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
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**
Data controllers and data processors

- **The pharmacy business/organisation = data controller**
- **Data controller** = a person (alone or multiple) who determines the why and how personal data is to be processed
- **Data processor** = a person (other than employee) who processes personal data on behalf of the data controller – e.g. *PMR supplier, external payroll or external courier company*
- Those working within the pharmacy organisation are **not** data processors
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 (DPIA) (where appropriate)
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

• Organisations must report data breaches to the ICO where there is a risk to the individual’s freedom and rights
  – Breaches must be reported within 72 hours
  – Fine dependent on infringement; up to either:
    – €10million or 2% of the organisation’s global turnover
    – €20million or 4% of the organisation’s global turnover

• In some cases, the organisation must contact the affected individual(s), NHS England, regulatory body or police
# Data breaches: examples

Report data breach to ICO if there is a risk to the individual’s rights and freedoms; determine on a case-by-case basis

<table>
<thead>
<tr>
<th>Internal data breaches</th>
<th>External data breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Unauthorised access of staff information – address, payroll, sickness log</td>
<td>• Unauthorised access to patient information – by cleaners with no confidentiality agreements</td>
</tr>
<tr>
<td>• Altering personal data without permission</td>
<td>• Taking in repeat prescription requests outside of pharmacy – such as in a supermarket</td>
</tr>
<tr>
<td>• Losing personal data of staff</td>
<td>• One prescription, or end of month bundle going missing/incorrectly delivered</td>
</tr>
<tr>
<td>• Absence of technical security measures leading to malware</td>
<td></td>
</tr>
</tbody>
</table>
Data Protection Officer (DPO)
DPO: requirements

• Under the GDPR, a DPO is required if an organisation carries out “large scale processing of special categories of data” or is a public authority

Public authority

Pharmacy organisations providing pharmaceutical services under contract to the NHS in England, Northern Ireland, Scotland and Wales, or by other arrangement with the public sector (for example, providing services commissioned by local authorities) are deemed a ‘public authority’ in respect of the processing of information related to those services
DPO: appointing

- Responsibility = data controller/processor
- **ICO**: DPO must act *independently* and be an *expert* in data protection law; advisable for them to have knowledge of the pharmacy sector
- If a DPO is appointed for *more than one* organisation, the size and structures of *all* organisations need to be considered to ensure how realistically that DPO can perform their duties/tasks
  - The DPO must have the *necessary resources* for support which may include a team to help them, as appropriate
  - The DPO is required to *be easily accessible* by the employees of each organisation
DPO: external or internal?

• ICO has stated that the DPO can be externally appointed
  – If externally appointed, duties, position and tasks assigned should be the same as an internally-appointed DPO

• ICO has 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
DPO: no conflicts of interest

- GPhC/PSNI: Pharmacy professionals must act honestly and professionally with integrity
- An existing pharmacy professional employee can act as DPO in-line with other duties such as superintendent
- An existing non-pharmacy professional employee can act as DPO as long as they demonstrate they will act in-line with DPO duties and requirements
DPO: GDPR Article 29 Working Party

• A DPO cannot **determine** the processing means and purposes

• However, due to the structure of certain organisations, this is to be considered on a **case-by-case basis**

• Therefore, data controllers/processors should **consider** the following when ensuring their appointed DPO has no conflicts of interest:
  
  – Identify roles within the organisation that are incompatible with the DPO role
  
  – Determine internal rules to avoid any conflicts of interest
  
  – **State justifications regarding conflict of interests** (e.g. When one man band then justify why no conflict of interest)
  
  – **Declare appointed DPO has no conflict of interest**
  
  – Ensure internal rules safeguards
  
  – Ensure the notice period for the DPO is precise and detailed to avoid conflict of interests
DPO: role

The DPO is **not** personally liable for complying with data protection law

- This responsibility lies with the data controller/data processor

However, DPO = **crucial role** in ensuring **compliance** with data protection obligations

If the organisation decides **not** to follow DPO’s advice, the justification must be clearly documented demonstrating the accountability lies with that organisation
DPO: training

- **No specific training** is required for the role of a DPO; however, the DPO is expected to have expert knowledge of data protection law and where possible, knowledge of pharmacy sector
  
  – Credentials are to be *proportionate* to type of processing, remembering the level of protection required (e.g. health data is high level)

- **NPA support** – a suite of resources and guidance documents specifically developed for DPOs and we will provide face to face support
DPO: relevant skills and expertise

- Expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
- Understanding of the processing operations carried out
- Understanding of information technologies and data security (NPA cyber security resource useful)
- Knowledge of the pharmacy sector and the organisation
- Ability to promote a data protection culture within the organisation

Ref: Article 29 WP guidance
Data controller/processor and DPO

Data controller/processor responsibility in appointing a DPO

- Ensure the DPO works independently
- Involve the DPO in a timely manner concerning all data protection matters
- Ensure the DPO has sufficient resources
- Ensure the DPO is not penalised
- Internal DPO: ensure no conflicts of interest
- Publish contact details for DPO to the ICO, employees and in privacy notice for customers/patients

DPO responsibility for undertaking the role and completing necessary tasks

- Provide advice, support and raise awareness on data protection obligations; consider risks involved within the context, nature, purpose and scope of the processing
- Monitor compliance to data protection laws and relevant policies
- Ensure audits and training are undertaken
- Advise and monitor Data Protection Impact Assessments (DPIAs)
- Report to the highest management level
- Act as a point of contact for organisation’s employees, ICO and data subjects
DPO: independent working

• Data controllers/processors cannot instruct DPO:
  – How to deal/investigate a complaint/matter
  – Whether or not to contact the ICO
  – To take a particular view/interpretation

• Data controllers/processors remain responsible for compliance; if DPO advice is not followed:
  – Document justification demonstrating the accountability lies with that organisation
  – DPO to directly report to highest level of management
  – DPO can choose to provide annual report of their activities
DPO: involvement

• Data controllers/processors: involve the DPO in a **timely manner** concerning all data protection matters
  – At the earliest possible stage
  – Especially when carrying out a DPIA

• Quick involvement ensures compliance with GDPR and promotes privacy by design approach

• Prompt involvement after a data breach or incident
DPO: adequately resourced

A DPO should be adequately resourced:

- **Senior management** to actively support
- **Sufficient time** provided for duties/tasks, especially if internally appointed – other non-DPO roles could result in DPO role neglect
- **Support** with equipment, facilities, premises, staff, other services (HR, IT, legal), as appropriate
- All employees to receive **official communication** of DPO designation
- **Continuous learning**: up-to-date with any developments, increase DPO expertise, participate in training courses/professional development
- Consider a **DPO team** (one person to be nominated as lead) considering size/structure of organisation
DPO responsibilities
DPO: responsibilities

• **Informs** and **advises** the organisation of GDPR requirements; this requires:
  – Taking into account the risks involved within the **context, nature, purpose and scope** of the processing
  – Provide advice that is risk-based: focus and prioritise high risk activities such as the processing of special categories of data

• Helps in internal **compliance monitoring**; this includes, advising and monitoring data protection impact assessments, data protection policies, managing data activities, raising awareness of data protection issues, training staff and undertaking internal audits

• Should be adequately **resourced** and involved in all matters concerning data protection

• **Reports** to the **highest management level** of an organisation
DPO: compliance monitoring

A DPO should:

• **Collect** information to identify processing activities
• **Analyse/check** compliance of processing activities
• **Advise, inform** and give **recommendations** to data controller/processor

! Remember: compliance responsibility lies with the data controller/processor – not DPO
DPO: data protection impact assessments

• **Data controller** is responsible to carry out a DPIA; however, DPO can play important/useful role in **assisting**

• Data controller **seeks DPO advice** on, amongst others:
  – Whether or not to carry out DPIA
  – What method to follow
  – Whether to conduct DPIA in-house or outsource it
  – What safeguards to apply to mitigate an individual’s freedoms and rights
  – Whether the DPIA has been correctly carried out
  – Whether the DPIA conclusions are in compliance with GDPR

• The **precise tasks** of DPO and scope to be **outlined** in the DPO contract in respect of carrying out a DPIA
Data protection impact assessments exceptions

• DPIA may not be required where data is processed:
  – To meet legal requirements (e.g. NHS contractual obligations)
  – In the performance of a task in the public interest
  – Where an assessment was previously carried out

• It is likely that most smaller pharmacies will not need to carry out a DPIA for regular dispensing

• However, a DPIA will be required when introducing new technologies to the pharmacy business – e.g. introducing a dispensing robot
DPO: ICO contact

- The DPO should **co-operate with the ICO** and **act as a contact point for the ICO on issues relating to processing and to consult, where appropriate, with regard to any other matter**
- DPO is bound by **confidentiality** and **secrecy**
- However, the DPO can contact ICO and seek advice as appropriate
- Additionally, the ICO can contact the DPO to fulfil its tasks, such as investigating
DPO: contact details

- Acts as a **point of contact** for the organisation’s employees, the ICO and the individuals whose personal data is processed by the organisation, therefore, their contact details should be **readily available**
  - Confidentiality is paramount
  - The DPO is bound by secrecy

- **Contact details** include: postal address, dedicated telephone number, dedicated email address

- **ICO**: must have name and contact details

- **Data subjects/employees**: contact details do not require DPO name; however, good practice to do so
Record keeping

- Data controller/processor **must** maintain records of processing (templates available)
- DPOs, **in practice**, hold records of processing based on information provided to them from the organisation
- Data controller/processor **can** assign the DPO with keeping records on their behalf
  - This could be considered as a tool to enable the DPO to perform their task of monitoring compliance and advising/informing the data controller/processor, as required
- Records should be made **available** to the data controller/ICO upon request
In a nutshell

- The DPO role needs to be differentiated from that of a data controller/processor
- The data controller/processor is required to appoint a DPO
- The data controller/processor is responsible for complying with data protection laws
- The DPO has a crucial role in supporting the data controller/processor to fulfil their data protection obligations
‘CONSENT’
Confusion over ‘consent’

- Clarity is required over the use of ‘**consent**’ as a lawful basis for processing personal data vs. the use of the word ‘consent’ when used in the context of obtaining **permission/authorisation** to permit the provision of a service to patients.

- It is advisable to consider one of the other five lawful bases for processing personal data wherever applicable and possible.

- ‘**Consent**’ as a lawful basis is **not** appropriate if it is a precondition for patients to access a service offered.
‘Consent’ as a lawful basis

When ‘consent’ is used as a lawful basis, it needs to be GDPR-compliant and meet the following criteria:

– Consent must be freely given.
– Consent should be obvious and require a positive action to opt in.
– Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.
– Consent must specifically cover the controller’s name, the purposes of the processing and the types of processing activity.
– Explicit consent must be expressly confirmed in words, rather than by any other positive action.
‘Consent’ as permission/authorisation

• Many services provided by community pharmacies require that ‘consent’ is obtained from the patient – for example, to receive a Medicines Use Review (MUR), to collect a patient’s prescriptions from their surgery, or to deliver medicines to them at home.

• In all these cases, ‘consent’ is deemed to be in the context of obtaining the patient’s permission/authorisation to carry out and/or provide the relevant service – It is not ‘consent’ in the context of the lawful basis for processing personal data under the GDPR.
How to prepare and NPA support
NPA DPO guidance

- Launched today
- The DPO guidance resources include:
  - **GDPR DPO guidance**: providing an overview on the roles and responsibilities of the data controller, data processor and DPO
  - **GDPR DPO checklist**: a template supporting the DPO to undertake their role helping the DPO give action/feedback to the data controller/processor on their compliance with data protection laws and relevant policies
  - **GDPR definitions and quick reference guide**: a go-to list of important definitions and quick reference guide which can be used by the DPO to help raise data protection awareness to those in the organisation
Data Protection officer (DPO) checklist for *(insert name of organisation)*:

<table>
<thead>
<tr>
<th>DPO name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of starting role:</td>
<td></td>
</tr>
<tr>
<td>Date of completing this checklist:</td>
<td></td>
</tr>
<tr>
<td>Report directly to:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DPO tasks</th>
<th>Action points, comments or further information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advise and inform the organisation (data controller/processor) of relevant data protection laws.</td>
<td></td>
</tr>
<tr>
<td>Advise and inform those working within the organisation of relevant data protection laws.</td>
<td></td>
</tr>
</tbody>
</table>
GDPR: NPA support

General Data Protection Regulation (GDPR): DPO resources
A suite of resources to understand the requirements of appointing a DPO and their role, the following documents are available:
- DPO guidance
- DPO checklist
- GDPR definitions and quick reference guide

General Data Protection Regulation (GDPR): brief overview
This resource provides a brief overview of the GDPR.

General Data Protection Regulation (GDPR): training manual and MCQs
To help comply with the GDPR requirement of staff awareness, the following documents are available:
- Pharmacy team training manual
- MCQ assessment
- MCQ assessment answers
- Certificate of completion

General Data Protection Regulation (GDPR): FAQs
Current FAQs on the GDPR.

General Data Protection Regulation (GDPR): lawful basis for processing
This resource provides a brief overview of the lawful basis for processing under the GDPR.

General Data Protection Regulation (GDPR): consent
A brief overview of consent as part of the GDPR and a template for prescription collection/delivery service

General Data Protection Regulation (GDPR): individual rights
This resource provides a brief overview on the rights for individuals and their personal data within the GDPR.

General Data Protection Regulation (GDPR): records of processing activities
A brief overview of records of processing activities and record templates for data controller and processors.

General Data Protection Regulation (GDPR): data breaches
This resource provides a brief overview of data breaches under the GDPR.

Your NPA represents, supports, protects
Welcome
This staff training manual has been produced by the NPA Pharmacy team to enable members of the pharmacy organisation gather an adequate understanding of the upcoming General Data Protection Regulation (GDPR).

The GDPR aims to standardise and simplify data protection rules and strengthen individuals’ rights in relation to their personal data.

A fundamental requirement for GDPR implementation is staff awareness. Pharmacy staff must have an understanding about the GDPR, its principles, and the roles, responsibilities and processes of organisations.

How to use this training manual
This training manual will help you understand the basis of the new regulation, and more importantly, provide you with information to help ensure compliance with the GDPR.

This training manual has been divided into the four following sections:
1. Introduction and background
2. Overview of the GDPR
3. Changes under the GDPR
4. Application of the GDPR

This training is expected to take 90 minutes to complete. It is recommended that you work through the training manual in the order presented.

Once you have worked through the training manual, you will be given a short multiple choice question (MCQ) assessment for you to complete to demonstrate your understanding of the GDPR.

After completing this training manual and associated MCQ assessment, it is recommended that you seek guidance from your employer, superintendent pharmacist or the person dealing with data protection within the pharmacy, to familiarise yourself with any additional policies and/or procedures which may be applicable to the pharmacy organisation.

Disclaimer:
As the information and guidance on the General Data Protection Regulation (GDPR) is constantly being updated, the contents of this training manual and any supporting resources may be subject to change. The information published is, to the best of our knowledge, correct at the time of publication. However, no responsibility will be accepted for any consequences of decisions made using this information.