General Data Protection Regulation (GDPR): lawful basis for processing – brief overview (March 2018)

***Disclaimer:* As the information on the General Data Protection Regulation (GDPR) is constantly being updated, the contents of relevant superintendent updates and 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.**

Introduction

The General Data Protection Regulation (GDPR) will come into effect in the UK from 25 May 2018. Many concepts and principles setting out the main responsibilities for organisations will be similar to the existing UK Data Protection Act 1998 (DPA); however, the GDPR will introduce new elements and significantly enhanced requirements regarding data protection. If an organisation needs to be compliant with the current DPA, it also needs to be compliant with the GDPR.

In preparation for the GDPR, the NPA has published a number of resources which can be downloaded from the NPA website.

This resource provides a brief overview of the lawful basis for processing under the GDPR.

Personal data processing: GDPR verses DPA

Personal data processing differs within the GDPR compared to the DPA; however, the concept of having a reason for processing personal data is not new.

- Under the DPA, organisations are required to choose a '*condition for processing*'
- Under the GDPR, this requirement is referred to as the '*lawful basis for processing*'; furthermore, the GDPR follows on from the DPA by placing a higher level of accountability and transparency on the chosen lawful basis for processing.

! All personal data must be processed **fairly**, **lawfully** and **transparently**. In addition, the lawful basis for processing chosen needs to be **demonstrated** that it is the most appropriate one.

Lawful basis for processing

Organisations need to identify and document their lawful basis for processing personal data, as well as the necessity for the processing. The lawful basis chosen will be dependent on the purpose for personal data processing and the relationship with the individual. If an organisation can reasonably meet the same purpose without processing the personal data, then a lawful basis does not exist – most of the lawful bases need a necessary reasoning for processing.

! **Necessary reasoning**: a business cannot simply state that personal data processing is necessary because of the way the business operates; the main question is whether personal data processing is necessary for the particular purpose

! **'Necessary' is not the same as 'essential':** the processing of data needs to be proportionate and targeted to achieving the purpose required – this does not mean that processing always has to be essential

Direct Dial: 01727 891 800 **Email:** pharmacyservices@npa.co.uk **Online:** www.npa.co.uk

General Data Protection Regulation (GDPR): lawful basis for processing – brief overview (March 2018)

A lawful basis **must** be determined before processing begins. If an incorrect lawful basis is initially chosen, this cannot be swapped to the correct one without good reasoning. If no lawful basis is relevant to the processing of particular data, then under the GDPR, it is unlawful for that data to be processed at all.

The lawful basis for processing personal data, and the reason for doing so, should be included in the **privacy notice** – this allows individuals to be informed of what data is being processed and why. If the purpose for processing personal data changes, the original lawful basis can continue to be used if it still applies, unless this was consent in which case the individual needs to provide new consent which explicitly outlines the new purpose, or another lawful basis needs to be chosen.

There are six lawful bases for processing data under the GDPR (GDPR Article 6):

a) *"the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;*

b) *processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*

c) *processing is necessary for **compliance with a legal obligation** to which the controller is subject;*

d) *processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;*

e) *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;*

f) *processing is necessary for the **purposes of the legitimate interests** pursued by the 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.*

Point (f)... shall not apply to processing carried out by public authorities in the performance of their tasks."

Processing special categories of personal data

If an organisation is processing special categories of personal data, a special condition is also required to be identified and recorded, along with one of the lawful bases – the lawful basis chosen does not dictate the special condition to be chosen; they do not need to be linked. The processing of special categories of personal data creates a more significant risk to an individual's freedoms and rights.

! **A pharmacy processes health data in their day-to-day practice which is a special category of personal data**

GDPR definition of "*processing of special categories of personal data*" (GDPR Article 9)

*"Processing of personal data **revealing racial** or **ethnic origin**, **political opinions**, **religious** or **philosophical beliefs**, or **trade union membership**, and the **processing** of **genetic data**, **biometric data** for the purpose of uniquely **identifying** a **natural person**, **data concerning health** or **data concerning a natural person's sex life** or **sexual orientation**".*

Direct Dial: 01727 891 800 **Email:** pharmacyservices@npa.co.uk **Online:** www.npa.co.uk

General Data Protection Regulation (GDPR): lawful basis for processing – brief overview (March 2018)

The GDPR identifies 10 conditions for processing special categories of personal data; however, additional conditions and safeguards will be introduced once the Data Protection Bill (currently passing through UK Parliament) comes into force.

GDPR special conditions for processing of special categories of personal data (GDPR Article 9)

a) *"the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;*

b) *processing is necessary for the **purposes of carrying out the obligations and exercising specific rights** of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;*

c) *processing is necessary to **protect the vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;*

d) *processing is carried out in the **course of its legitimate activities** with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;*

e) *processing relates to personal data which are **manifestly made public** by the data subject;*

f) *processing is **necessary for the establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;*

g) *processing is necessary for **reasons of substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;*

h) *processing is necessary for the **purposes of preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*

i) *processing is necessary for **reasons of public interest** in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;*

j) *processing is necessary for **archiving purposes in the public interest**, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."*

Direct Dial: 01727 891 800 **Email:** pharmacyservices@npa.co.uk **Online:** www.npa.co.uk

General Data Protection Regulation (GDPR): lawful basis for processing – brief overview (March 2018)

Example scenarios of processing special categories of data in a pharmacy setting highlighting the lawful basis of processing and the special condition for processing the special category of data, include:

- **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"*
  - **Special condition**: processing of the special category of data is necessary for *"...the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards…"*

- **Safeguarding vulnerable adults and children**
  - **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"*
  - **Special condition:** processing of the special category of data is necessary for "…*the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of ... social protection law in so far as it is authorised by Union or Member State law..."*

Complying with the GDPR

Although similar in nature, an existing DPA condition for processing needs to be checked to determine whether it still applies – in most instances, this will not change. Upon review, if a new lawful basis is required as the DPA condition is no longer appropriate, this is a chance to change the way personal data is processed to ensure compliance with the GDPR before it comes into effect on 25 May 2018. It should be noted that more than one lawful basis for processing may apply, and if this is the case, this should be clearly documented from the beginning.

! **Before GDPR comes into effect:**

- The lawful basis for processing activities must be clearly documented to demonstrate compliance
- All individuals involved must be informed of the lawful basis under which their data is being processed – this includes creating/updating privacy notices as necessary

! **Once GDPR comes into effect on 25 May 2018:**

- It will not be easy to switch between the lawful basis for processing and you will be breaching the GPDR if an appropriate lawful basis is not determined before it comes into play

Individuals rights regarding lawful basis for processing

The GDPR identifies that an individual has **eight rights** (refer to the NPA GDPR brief overview on individual rights). Individual rights under the GDPR can be affected depending on the lawful basis for processing chosen by an organisation. Table 1 details how individuals can be affected.

Direct Dial: 01727 891 800 **Email:** pharmacyservices@npa.co.uk **Online:** www.npa.co.uk

General Data Protection Regulation (GDPR): lawful basis for processing – brief overview (March 2018)

Table 1: how the lawful basis for processing can affect an individual's right

Lawful basis for processing	Individual's right		
	...to erasure	...to object	...to portability
Consent	✓	×*	✓
Contract	✓	×	✓
Legal obligation	×	×	×
Vital interests	✓	×	×
Public task	×	✓	×
Legitimate interests	✓	✓	×

**Individuals do not have the right to object to their data being processed where they have provided consent for processing – individual's do however have the right to withdraw consent*

Top tips: lawful basis for data processing under the GDPR

- ✓ Familiarise themselves with, and be aware of, the six lawful bases by which personal data can be processed under the GDPR
- ✓ Familiarise themselves with, and be aware of, the 10 special conditions for the processing of special categories of data under the GDPR
- ✓ Ensure a robust system is in place to undertake obligations under the GDPR – the Information Commissioner's Office has developed templates which can be used
- ✓ Ensure documented evidence of processing activities is kept to demonstrate compliance with the GDPR
- ✓ Check current and existing procedures relating to confidentiality, electronic records, information governance and record keeping in the organisation for processing activities
- ✓ Ensure all consent forms, privacy notices, records of personal data breaches are up-to-date

Reference, further reading and information

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- ICO "*Guide to the General Data Protection Regulation (GDPR)*": https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

Direct Dial: 01727 891 800 **Email:** pharmacyservices@npa.co.uk **Online:** www.npa.co.uk