Interim guidance notes on UK data protection in post-marketing pharmacovigilance

Pharmaceutical Information and Pharmacovigilance Association (PIPA)

Approval Status

Authors: PIPA
Version: 2.0
Date: 25 May 2018

Acknowledgments: We thank the many stakeholders from industry, regulators and professional organisations who have contributed, and will continue to contribute, to this guidance - including Bonelli Erede for the 2018 edition & pvlegal for the 2013 edition - and all those who provided feedback in response to our consultation on the 2017 revision of this guidance document.
# Table of contents

1. **Introduction**  
   1.1 Legislative background  
   1.2 Personal data in pharmacovigilance  
   1.3 Scope  

2. **Receipt of pharmacovigilance data and follow-up**  
   2.1 Collection and Receipt of data  
   2.2 Follow-up of pharmacovigilance data  

3. **Data entry and data transfers**  
   3.1 Data entry – fair and lawful processing  
   3.2 Data entry – security and use of third parties  
   3.3 Data entry and international data transfer  

4. **Access, rectification and objection rights**  
   4.1 Access to personal data  
   4.2 Responding to a data subject access request  
   4.3 Rectification, blocking, erasure and destruction of personal data  
   4.4 Objection to processing personal data  

5. **Retention and redaction of personal data**  
   5.1 Redacting personal data  
   5.2 Personal data relating to patients  
   5.3 Healthcare professional personal data  
   5.4 Sharing safety information with business partners and vendors  
   5.5 Retention period  

6. **Security**  
   6.1 Pharmacovigilance data  
   6.2 Use of third party vendors  

7. **Notification**  

**Annex 1:** Abbreviations  
**Annex 2:** Definitions  
**Annex 3:** Sample data protection notices  
**Annex 4:** Options for establishing adequacy and DPA exemptions  
**Annex 5:** Access to personal data
1. Introduction

This interim guidance is provided only for guidance purposes and is not legally binding. It seeks to achieve the use of best practice in the pharmaceutical industry regarding post-marketing pharmacovigilance reporting. This interim guidance may be used to develop and to both inform and monitor your company’s policies and procedures.

It has been prepared by the Pharmaceutical Information and Pharmacovigilance Association (PIPA) to help companies performing post marketing pharmacovigilance (PV) in the UK to meet their data protection obligations under the UK Data Protection Act (DPA) 1998, as amended by the UK Data Protection Act 2018.

This interim guidance may be provided to the Information Commissioner’s Office (ICO) for their awareness. The ICO may issue its own guidance for related purposes in the future.

This document does not consider data protection requirements in countries outside the UK and does not consider laws or regulatory requirements outside of data protection which may also apply to the use and retention of PV data.

1.1 Legislative background

In the United Kingdom, the DPA governs the processing of personal data and implements EU Directive 95/46/EC (the Data Protection Directive).

The DPA and the Data Protection Directive will be amended no later than the entry into force of the European General Data Protection Regulation (GDPR): Regulation (EU) 679/2016\(^1\). The GDPR was adopted on 24 May 2016 and came into force on 25 May 2018.

**Key changes introduced by the GDPR are:**

- **Territorial scope:**

  The GDPR applies in and outside of the UK, and outside of the European Union\(^2\)

- **Definition of health data**

  “personal data related to physical or mental health […] which reveal information about his or her health status”

  Genetic data is also now considered to be treated as sensitive data, though it is not classified as health data of itself.

- **Processing of health data:**

  Health data, together with other sensitive data, are subject to a general prohibition on processing without informed consent, unless an exception applies.

---


\(^2\) Article 3(2) (b) “This Regulation applies to the processing of personal data …. by a controller or processor not established in the Union...”
However, Article 9(2)(i) recognizes that processing of data is necessary to fulfil pharmacovigilance obligations.

**Article 9 (2) (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 law or Member States law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subjects, such as professional secrecy”.

- **Pseudonymisation (Article 4 (5) GDPR)**

Pseudonymisation: “means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information”

- **Anonymisation (Recital 26 GDPR)**

In this recital, this is described as “Data rendered anonymous in such a way that the data subject is not or is no longer identifiable”

This can be compared to the ICO’s definition, which is wider to the terms of Recital 26, with the addition of the word ‘likely’:

“Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place”.

- **Sanctions**

GDPR has introduced new sanctions for infringements of its fines (up to 4% annual global turnover) and new legal remedies (class actions) for infringements of regulations.

**Brexit and UK Implementation of data privacy law**

As of May 2018, the UK is expected to cease to be a member of the European Union in 2021.

The Data Protection Act 2018 received Royal Assent on 23 May 2018 and its main provisions came into force on 25 May 2018.

It sets out derogations from the GDPR (those are areas where Member States can decide to introduce alternative provisions, such as exemptions from GDPR). It includes other national implementing measures, such as an extension of the ICO’s powers. For example, it sets out extended powers for the ICO to levy fines of up to £17million or 4 per cent of global turnover on organisations that breach the DPA.

The new Act brings the GDPR requirements into UK law and extends it to cover legal areas for which the EU does not have oversight. It will remain in force even after the UK leaves the EU.

The ICO has published a summary of the Data Protection Act 2018

*Companies should anticipate that further guidance on the implementation of the GDPR and*

---

3 In Recital 26 GDPR, it is stated that data which “has undergone pseudonymisation”, but still could be attributed to a natural person by the use of additional info, should be considered to be personal data.
DPA 2018 may be provided after 25 May 2018 from relevant regulatory authorities. Companies should also check guidance on technical standards for use of Apps published by the MHRA and the NHS.

The DPA uses a number of defined terms which are used in this guidance and which are set out in Annex 2.

The DPA applies to the processing of personal data by a data controller established in the UK or, if not established in the UK or any other European Economic Area (EEA) State, uses equipment in the UK for processing personal data (other than for the purpose of transit of personal data through the UK). A pharmaceutical company processing personal data for PV will act as a data controller (see Annex 2 for definitions).

The ICO monitors compliance of the DPA and GDPR and can enforce compliance through criminal prosecution, non-criminal enforcement, audits and also has power to serve a monetary penalty notice on a company in cases of serious breaches of the DPA principles.

The DPA has general applicability and is not specific to the pharmaceutical sector. This guidance has been developed to assist companies with meeting UK data protection requirements when conducting PV activities.

1.2 Personal data in pharmacovigilance

Introduction

Two types of data are subject to regulation:

- personal data received through the collection of reports (email addresses, phone numbers etc.)
- the data that no longer contains personal data, for processing

Information about patients must be collected, processed, stored and reviewed by companies when carrying out PV to ensure the safety of patients and to comply with strict obligations to report suspected adverse reactions to regulatory authorities. Companies may be subject to civil proceedings and criminal enforcement if they fail to fulfill their PV duties.

PV data may include personal data and sensitive personal data related to the patient, who is the subject of the case, and personal data related to the reporter, who may be the patient’s healthcare provider, family member or the patient themselves (see Annex 2 for definitions).

A patient’s age/age group, sex, weight, height, ethnicity, medical history and status are required for effective safety data analysis.

A patient’s initials or an assigned ID and/or date of birth are important to identify duplicates, and the reporter’s name and contact details are needed to perform effective follow-up to ensure that complete and accurate data are collected.

In PV, patient identifiers and other adverse event data may amount to personal data. The EU

---

6 See EMA Press Release 4 July 2016
Data Protection Directive and the GDPR state that whether or not an individual is identifiable depends on all the means likely to be reasonably used to identify them.

The European Data Protection Supervisor (EDPS) is of the view that PV data should in principle be considered personal data and for practical purposes this guidance considers that PV data should be treated as personal data. PV data relating to the health of a patient is generally considered sensitive personal data. In 2013, the EDPS addressed vigilance marketing surveillance and reporting in an opinion on new regulations on devices. The EDPS considers patients should give consent for processing of their personal data, and that surveillance should be carried out using anonymous data.

Companies must comply with the DPA when processing personal data for PV and have transparent and robust processes in place.

Regular training in data protection requirements is recommended for all company staff involved in PV activities.

The DPA will also expect agreements that implement PV duties to include clauses to address the protection of personal data. For example, in July 2017 the MHRA reminded companies to follow Good Distribution Practice - GVP Module VI.2.2. This states that “Each marketing authorisation holder shall have in place a system for the collection and recording of all reports of suspected adverse reactions which are brought to its attention”. Such a system would usually be implemented by a clear and detailed agreement with procedures and associated training. They must include clauses to comply with the DPA.

**Anonymisation/Pseudonymisation**

The ICO supports appropriate anonymisation and produced a Code of Practice on anonymisation for all sectors. The ICO also supports the UK Anonymisation Network.

The ICO considers there is no need to request consent for anonymisation.

There is much debate on whether pseudonymisation is a suitable alternative to anonymisation. Partly for this reason, the EMA has set up a cross-functional Technical Anonymization Group of experts that should publish its view in 2018. It will consider encryption and possibly in what circumstances it is appropriate to unlock encryption.

The GDPR also requires those who choose to pseudonymise data, to ensure that the “additional information” (used to pseudonymise) is “kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person.”

*Most companies already anonymise personal data on a global basis & adopt secure forms of encryption to reduce intrusion by hacking.*

---

10 [http://ukanon.net/](http://ukanon.net/)
11 In Ireland: [https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm](https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm)
Other guidance

- Patient Registries

After a Patient Registries Workshop in October 2016, in February 2017 EMA published the following recommendations regarding PV & data protection\(^\text{12}\) (see Chapter 3.5.2):

> “Procedures need to be developed and implemented by registries in order to safeguard core principles such as transparency, accessibility of data for public health purposes and independence. Guidance or clarification documents may be needed from regulators, for example in the area of reporting of adverse events/adverse drug reactions”.

- ISPOR Code of Ethics 2017

Safety / (Serious) Adverse Events\(^\text{13}\)

> The balance of risk or harm to benefit for patients must be considered in HEOR studies, and must be communicated to patients via informed consent.

1.3 Scope

This guidance applies to PV data processed in the post marketing setting for which there may be no explicit consent from the data subject for processing of their personal data (generally products under Module VI of the EMA Good Vigilance Practice Guidance)\(^\text{14}\).

Activities performed as part of a clinical trial (under Volume 10)\(^\text{15}\) or other company activities where there is explicit consent from the data subject for processing their personal data are not in scope. Guidance for the secondary use of data for medical research is covered separately\(^\text{16}\).

2. Receipt of pharmacovigilance data and follow-up

2.1 Collection and Receipt of data

Companies collect data using a variety of tools and sources. The MHRA and EMA anticipate use of social media and apps for this purpose.

Companies should check that these tools have provided adequate information to patients as to


\(^{13}\) At line 275 - [https://www.ispor.org/ISPOR_Code_of_Ethics_2017-Final_Draft_for_Review.pdf](https://www.ispor.org/ISPOR_Code_of_Ethics_2017-Final_Draft_for_Review.pdf)


\(^{16}\) ABPI 2007. ABPI guidelines for the secondary use of data for medical research purposes. Available at: [www.abpi.org.uk/our-work/library/guidelines/Pages/secondary-use-data.aspx](http://www.abpi.org.uk/our-work/library/guidelines/Pages/secondary-use-data.aspx)
how certain data including cookies may be used for PV activities.

When an AE is reported to a company it is important that some personal data is collected to meet the PV requirements of having an identifiable patient and reporter.

Module VI, section VI.B.2 of the Good Vigilance Practice Guidance\(^\text{14}\), requires that companies ensure individual case safety reports (ICSRs) contain a minimum set of information. It also specifies that information relating to the patient is as complete as possible, in accordance with local privacy laws.

Regardless of whether a data subject is the person who has suffered an AE or is a person reporting the AE (e.g. a healthcare professional (HCP) or a patient’s relative), it is not necessary to obtain consent from the data subject in order to process personal data relating to the data subject for the purposes of PV\(^\text{17}\). This is because it is the ICO’s view that it should be possible to rely on the medical purposes legal ground in the DPA to process PV data that is sensitive personal data.

However, data subjects (persons who have experienced an AE and if different, the persons making the AE reports) must understand what personal data relating to them is being collected, by whom and for what purposes. Data subjects should be informed of who will receive their personal data; it should be sufficient to generally identify them (e.g. health authorities) rather than naming individually. This information should be set out in a clearly written data protection notice (DPN) that can be easily understood. Any DPN for the EU needs to include a reference that information may be included in the EMA’s EudraVigilance database\(^\text{18}\).

Data subjects should be allowed to give their consent. GDPR notes that this could be given as a written statement, including by electronic means, or by oral statement. If the report is received by phone, verbal consent should be requested and recorded. However, an attempt should then be made to obtain written consent from the data subject. If the data subject does not give consent for their personal data to be recorded, a company should consider what limited information it will retain to comply with its PV obligations. This could include anonymised data for the patient identifier such as patient initials, age or gender, drug and event.

Different channels of AE reporting to a company may require different DPNs (see Annex 3). If a company is unable to provide a DPN directly to the person who has suffered an AE because the AE report is made by a HCP, we recommend use of a statement like the one below, to remind the reporter of his/her obligation under the DPA to notify patients when a disclosure of personal data is made:

\textit{We advise that all patients are informed in writing (by letter or by e-mail with acknowledgment of receipt) if an adverse event has been reported that relates to them. If it is not possible to write to a patient, a company should document the reasons for this.}

\(^\text{17}\) In order to process personal data, a company must meet the conditions of the DPA. Personal data for PV may be processed on the basis that processing is necessary for compliance with any legal obligation (paragraph 3 of schedule 2 DPA) and for the purposes of legitimate interests pursued by the data controller (paragraph 6 of schedule 2 DPA). Sensitive personal data may be processed where the processing is necessary for medical purposes and undertaken by an HCP, or a person who owes a duty of confidentiality which is equivalent to that which would arise if they were an HCP. Medical purposes includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services (paragraph 8, schedule 3 DPA).

\(^\text{18}\) EMA/759287/2009 Rev 3. European Medicines Agency policy on access to EudraVigilance data for medicinal products for human use
2.2 Follow-up of pharmacovigilance data

All correspondence with a reporter needs a DPN; text in Annex 3 can be added to company follow-up request forms or AE forms sent to a reporter for completion.

Consent should always be obtained from a patient in writing to follow up with their HCP. It is a company decision how this is obtained and documented.

3. Data entry and data transfers

3.1 Data entry – fair and lawful processing

Data entered into safety databases must only be processed for PV purposes and should not be processed for purposes not disclosed to the data subject.

Companies should be able to justify why they retain data for a specific period of time (see Section 5).

3.2 Data entry – security and use of third parties

Companies must put in place appropriate measures against unauthorised or unlawful processing of personal data and accidental loss, destruction or damage to personal data.

Such measures should include taking reasonable steps to ensure the reliability of employees who have access to personal data and to ensure employees receive adequate training on the lawful processing of personal data.

Responsibility to ensure appropriate security measures are in place remains with companies when outsourcing data entry or other processing activities to third parties. Companies must ensure such third parties provide similar measures to those described above and take reasonable steps to ensure compliance.

Companies must enter into a written contract which obliges third parties (that act as data processors) to only process personal data on company instructions and to provide adequate security for the processing of personal data, see Section 6 for further details.

3.3 Data entry and international data transfer

PV data entry in the UK may involve entering personal data into safety databases which can be accessed by companies, service providers or third parties outside the EEA. Entering PV data in a database hosted outside the EEA, or which can be accessed outside the EEA, will amount to a transfer of personal data outside the EEA for the purposes of the DPA.

If PV data that is personal data, is hosted, or backed up outside the EEA, this is considered a transfer of personal data from the EEA even if the PV data cannot be viewed outside the EEA. If the global safety database is hosted in the UK, the DPA applies regardless of where the personal data was received or where the database is accessed. The DPA will also apply where a global safety database containing personal data is hosted outside the UK where the company is established in the UK.
It is prohibited to transfer personal data outside the EEA unless the country or territory of receipt ensures an adequate level of protection for the rights of data subjects in relation to processing of personal data.

Where there is a transfer of personal data to a country outside the EEA not considered by the European Commission to provide adequate protection, a company can put in place arrangements deemed to provide adequate protection for processing personal data. In addition, the DPA provides some limited exemptions to the prohibition on international transfers, see Annex 4.

Companies should consider if existing data transfer solutions can be relied on for transferring PV data. Where no appropriate existing solution is in place, a data transfer solution should be implemented from the EEA or otherwise either:

- limit transfers so PV data can only be accessed in the EEA, or
- make data anonymous before transfer\(^\text{19}\).

The same data protection principles apply when transferring to regulatory authorities outside the EEA.

### 4. Access, rectification and objection rights

#### 4.1 Access to personal data

A Data Subject has the same rights to access PV data as any other personal data\(^\text{20}\) (see Annex 5). These rights include the right for individuals to update the information.

#### 4.2 Responding to a data subject access request

In the UK, access needs to be requested in writing (email is acceptable). Under the DPA 1998, an access request was subject to a maximum £10 fee, although companies were under no obligation to charge. Under GDPR, no fee should be charged, unless the requests from a data subject are manifestly unfounded or excessive.

An individual only has access rights to personal data which relates to them and companies should take reasonable steps to verify the identity of the person making the request (a person may make a request via a third party in which case the company needs to be satisfied the third party is entitled to act on behalf of the individual). Companies have no obligation to provide personal data if not satisfied as to the identity of the requestor.

The information supplied must be understandable to the person making the request, for example, technical terms and abbreviations should be explained.

---


It is advisable that data subject access requests are handled in conjunction with the company Legal Department and/or Data Privacy Officer.

Under the 1998 DPA, companies had 40 days to respond to a request from the date of receipt. If a fee was charged and/or more information was required from the requestor to identify the data subject or the location of the personal data, the 40-day period started to run from the date on which both the fee (if one is applied) and the additional information had been received. It is important to note that these timelines have been reduced to 30 days, under GDPR and one month under the 2018 DPA.

Reminder: companies do not have the full identity of a patient if reports are received from a HCP. For these reports, the patient access or rectification request shall be done through the HCP.

4.3 Rectification, blocking, erasure and destruction of personal data

The law requires that personal data held by a company is accurate and where necessary kept up to date. If an individual challenges the accuracy of information held about them, the information should be amended or deleted assuming there is no reason to question the accuracy of the new information.

PV source documentation should not be destroyed, even if requested by a data subject (except for any personal data that can be used to identify the data subject). Such documentation is to be retained, and not redacted.

If an individual is not satisfied that information held about them is accurate, they can apply for a court order that the company rectify, block, erase or destroy the information.

4.4 Objection to processing personal data

A person has a right to object to their personal data being processed only if the processing causes, or would be likely to cause, unwarranted substantial damage or distress. If the processing is being performed to fulfil a legal obligation for PV, then while a company must respond to such a request they are not obliged to comply with it.

A company is required by law to collect certain minimum information relating to persons who have suffered an adverse event or potential adverse reaction to the company’s medicinal product in order to monitor the safety of its medicinal products.

5. Retention and redaction of personal data

The DPA requires that companies should not hold more personal data than is needed for the particular processing activity and that data should not be kept longer than necessary for the purposes of the processing. The DPA also requires that personal data is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed.

---


5.1 Redacting personal data

Companies should practice ‘data minimisation’ i.e. identification of the minimum amount of personal data needed to properly fulfil their safety reporting activities. A company should not de-identify or redact personal data if its PV obligations are compromised by doing so.

5.2 Personal data relating to patients

When determining whether to redact elements of personal data, companies should consider whether there is a legitimate reason for keeping the data in the safety database - such as identification of duplicates and performing follow-up activities.

Elements recommended for retention for effective PV: patient initials or ID, gender, date of birth, age/age group at onset, ethnicity and the adverse experience: symptoms, outcome, duration, suspect drug, medical history, concomitant medication.

Elements recommended for redaction (not usually required for effective PV): patient name, contact details (address, telephone, email address) and hospital number. Companies should consider removing elements not required for PV from source data e.g. by removing with black marker from paper or via the Adobe Redact function for scanned in records and not entering names and addresses into databases. If the patient is also the reporter or the only source of obtaining follow-up information, it is acceptable to retain this information.

5.3 Healthcare professional personal data

It is advisable to retain HCP data, such as name and contact details once follow-up activities are complete, should the need arise to revisit AEs reported.

5.4 Sharing safety information with business partners and vendors

Only information which the recipient reasonably needs, and which is consistent with the purpose of PV, should be transferred when forwarding an AE report to another company. As mentioned in Section 2.1 above, the DPN should provide details of the recipients.

5.5 Retention period

Article 12 of the European Commission’s PV Implementing Regulation states that product-related documents be retained as long as the marketing authorisation (MA) exists and for at least 10 years after the MA has ceased to exist. 23

Source safety documentation containing personal data received by non-PV departments and held in their databases should be managed in the same way as the PV department.

Companies should ensure contracts with business partners and vendors specify requirements for retention of PV documents and that PV documentation is not destroyed without notification to the other party.

---

6. **Security**

6.1 **Pharmacovigilance data**

Companies are required to take appropriate measures against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage\(^{24}\).

Documentation containing PV data should not be left unattended and companies should adopt a clear desk policy for PV documents. Hard copies of documents, including those in workflow progress should be stored in a secure and robust area such as fire-retardant cupboards/archives.

Any database containing personal data used in PV should be fully validated or tested, as appropriate, to ensure changes to data can be identified and access to these systems should be restricted to named individuals. Companies may also consider configuring PV databases to restrict access to sensitive personal data so only the country of collection has access, although this is not a requirement of the law.

Sensitive data should be encrypted to ensure the integrity of data transmissions.

6.2 **Use of third party vendors**

See Section 3.2

7. **Notification**

A pharmaceutical company processing personal data must, subject to limited exceptions, notify the ICO of its personal data processing activities yearly. One notification per company is required covering all its data processing activities, including processing performed for PV. The ICO makes certain details of each notification public via its Data Protection Public Register\(^{25}\).

Notification should be made using the standard notification form available at [www.ico.gov.uk](http://www.ico.gov.uk).

To assist companies, various fields in the standard notification form contain a menu of options. The ICO has pre-specified a number of standard purposes for which companies may process personal data and has provided a description of each. The list includes: ‘health administration and services’ and ‘research’.

Companies may select one of these general descriptions to cover processing for PV or alternatively, add ‘pharmacovigilance’ as an additional purpose to the notification form together with a short purpose description e.g.:

*Coffee, monitoring, researching, and evaluating information from healthcare providers and patients on the adverse effects of medicines.*

The pre-specified menu options for recording the type of data subjects, classes of personal data

---


processed and recipients to whom personal data are disclosed should be sufficiently comprehensive for the majority of companies.

If a change to personal data processing arrangements means a company’s register entry is no longer current, the change must be notified to the ICO as soon as possible but in any event within 28 days.

Failure to notify or to renew the notification and failure to keep notification information up-to-date are criminal offences.
Annex 1: Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AE</td>
<td>Adverse Event</td>
</tr>
<tr>
<td>AOR</td>
<td>Acknowledgement of Receipt</td>
</tr>
<tr>
<td>BCR</td>
<td>Binding Corporate Rules</td>
</tr>
<tr>
<td>DPA</td>
<td>UK Data Protection Act</td>
</tr>
<tr>
<td>DPN</td>
<td>Data Protection Notice</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EMA</td>
<td>European Medicines Agency</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>HCP</td>
<td>HealthCare Professional</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioner’s Office</td>
</tr>
<tr>
<td>ICSR</td>
<td>Individual Case Safety Report</td>
</tr>
<tr>
<td>MA</td>
<td>Marketing Authorisation</td>
</tr>
<tr>
<td>MAH</td>
<td>Marketing Authorisation Holder</td>
</tr>
<tr>
<td>MHRA</td>
<td>Medicines and Healthcare products Regulatory Agency</td>
</tr>
<tr>
<td>PIPA</td>
<td>Pharmaceutical Information and Pharmacovigilance Association</td>
</tr>
<tr>
<td>PV</td>
<td>Pharmacovigilance</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>WP</td>
<td>Working Party</td>
</tr>
</tbody>
</table>
Annex 2: Definitions

The DPA uses a number of defined terms; definitions based on the DPA which are also used in this guidance are set out below.

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anonymisation</strong></td>
<td>The process of turning data into a form which does not identify individuals and where identification is not likely to take place.</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td>Information that is processed by means of equipment operating automatically, including data that is recorded with the intention of being so processed or is recorded as part of a relevant filing system (e.g. structured paper files) or forms part of an ‘accessible record’ which includes a record relating to the health of an individual and made by or on behalf of a healthcare professional.</td>
</tr>
<tr>
<td><strong>Data Controller</strong></td>
<td>Any person (either alone or jointly or in common with other persons) who determines the purpose for which, and the manner in which, any personal data are processed. This is often the company.</td>
</tr>
<tr>
<td><strong>Data Processor</strong></td>
<td>Any person, other than the data controller’s employees, who processes personal data on behalf of the data controller.</td>
</tr>
<tr>
<td><strong>Data Subject</strong></td>
<td>An individual who is the subject of personal data and who is living and identifiable; this could include, for example, patients, relatives of patients and HCPs.</td>
</tr>
<tr>
<td><strong>Personal Data</strong></td>
<td>Data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession of (or likely to come into the possession of) the data controller. This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.</td>
</tr>
<tr>
<td><strong>Pseudonymisation</strong></td>
<td>See Article 4(5) GDPR</td>
</tr>
<tr>
<td><strong>Sensitive Personal Data</strong></td>
<td>Data on racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, commission or alleged commission of a criminal offence.</td>
</tr>
<tr>
<td><strong>Processing</strong></td>
<td>Covers virtually anything that can be done with the data such as, but not limited to, organising, adapting, altering, retrieving, consulting, use, disclosure, transmission, dissemination, combining, blocking, erasure or destruction.</td>
</tr>
<tr>
<td><strong>Relevant Filing System</strong></td>
<td>Any set of information that is processed manually and is structured by reference to individuals or by reference to criteria relating to individuals so that specific information relating to a particular individual is readily accessible. See definition of ‘data’ above to determine what information is considered data under the DPA.</td>
</tr>
</tbody>
</table>
Annex 3: Sample data protection notices

The sample DPNs below are examples and should be modified to take into account the particular circumstances, such as the recipients of any PV data, and after having taken legal advice where necessary.

**Telephone**

Where a call is taken by a department designated to receive AEs, the following applies.

Acknowledge the person is reporting an AE and provide a DPN before processing any personal data such as:

*All the information and personal data you will share with us during this telephone conversation will be protected and kept confidential in line with [COMPANY SOP or POLICY] and local regulations. The information you provide will be used for the purpose of drug safety surveillance [and to enable us to deal with your enquiry appropriately] and it may be shared with health authorities. You have a right of access to your personal data which we hold about you.*

Where a call is received by other departments in error, the person answering the phone needs to acknowledge that the person is reporting an AE and explain that they are not the relevant person to talk to but they will take some details from the caller so that the correct person can call them back or transfer the call. If any personal data are processed, a DPN must be provided; this need only be given once.

In smaller companies or affiliate offices, calls may not be taken directly by the relevant department/person. The person answering the phone must acknowledge that the caller is reporting an event, explain they are not the relevant person to talk to and that they will take a message so the correct person can call them back.

Outgoing voicemail messages, especially outside of business hours, should provide the DPN, and direct the caller to leave a message and confirm that:

*All the information and personal data you will leave in your voicemail will be protected and kept confidential in line with [COMPANY SOP or POLICY] and local regulations. The information you provide will be used for the purpose of drug safety surveillance [and to enable us to deal with your enquiry appropriately] and it may be shared with health authorities. You have a right of access to your personal data which we hold about you.*
Email

An Acknowledgment of Receipt (AOR) needs to be sent back to the sender via email including a DPN. Outside of business hours, in addition to stating this is an automated reply, companies can consider using the same automated AOR and DPN:

Note:- information may be included in the EMA’s EudraVigilance database

All the information and personal data you will share with us on email will be protected and kept confidential in line with [COMPANY SOP or POLICY] and local regulations. The information you provide will be used for the purpose of drug safety surveillance [and to enable us to deal with your enquiry appropriately] and it may be shared with health authorities. You have a right of access to your personal data which we hold about you.

Face to face (i.e. sales force customer meetings)

Companies are obliged to train all staff to be aware what an AE is and what to do with the information when they are in receipt of one. Staff need to also assure customers that their personal data is treated appropriately:

All the information and personal data you have provided to me today will be protected and kept confidential. The information you provide will be used for the purpose of drug safety surveillance [and to enable us to deal with your enquiry appropriately].

Digital media

Company sponsored (controlled) digital activity – where AEs can be reported either via a ‘contact us’ page or from an ‘AE reporting’ link should have a DPN:

All the information and personal data you share with us in your enquiry information will be protected and kept confidential in line with [COMPANY SOP or POLICY] and local regulations. The information you provide will be used for the purpose of drug safety surveillance [and to enable us to deal with your enquiry appropriately] and it may be shared with health authorities. You have a right of access to your personal data which we hold about you.

This notice can appear on the website home page or as a pop-up prior to the AE being transmitted via the website.

Non-company sponsored (non-controlled) websites: Companies cannot put their DPN on a website they do not control. However, any messages received via a non-company sponsored website with contact information should be treated as having been received via email.

---

26 The European Data Protection Supervisor (EDPS) in an opinion in 2009 relating to the EMA stated that the notice should refer to transfers of data to the EMA and use of the data in EudraVigilance. European Data Protection Supervisor 2009 Opinion on a Notification for Prior Checking Received from the Data Protection Officer of the European Medicines Agency (“EMEA”) regarding the EudraVigilance database. Available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/ adequacy/index_en.htm
<table>
<thead>
<tr>
<th>Enquiries/report for non-company products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Companies are under no obligation to provide information on products that are not on their product portfolio. How staff handle these enquiries is a company decision. Companies may assist callers in obtaining contact details for the relevant company.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Follow-up of pharmacovigilance data</th>
</tr>
</thead>
<tbody>
<tr>
<td>All correspondence with a reporter will need a DPN. The notice below can be added to company-specific follow-up request forms or AE forms sent to a reporter for completion:</td>
</tr>
</tbody>
</table>

   *All the information and personal data you share with us will be protected and kept confidential in line with [COMPANY SOP or POLICY] and local regulations. The information you provide will be used for the purpose of drug safety surveillance [and to enable us to deal with your enquiry appropriately] and it may be shared with health authorities. You have a right of access to your personal data which we hold about you.*
Annex 4: Options for establishing adequacy and DPA exemptions

The DPA prohibits the transfer of personal data to a country outside the EEA that does not ensure an adequate level of protection for the rights of data subjects in relation to processing of personal data, unless certain derogations apply.

### Making a determination of adequacy

For transfers from the UK, it may be possible to transfer personal data outside the EEA where in the company’s view there is an adequate level of protection for the personal data to be transferred.

According to above ICO guidance, it is necessary to consider the type of transfer involved and whether this enables any presumption of adequacy. It is then necessary to consider and apply a so called ‘adequacy test’.


### Model Contracts

These are standard contracts which if entered into and complied with by both the exporter and recipient of personal data will be deemed to provide adequate protection for transferred personal data. There are two forms under the EU’s standard contractual clauses for transfer of personal data to third countries available for:

(i) transfers between a data exporter who is a data controller and a data importer who is a data controller and  
(ii) transfers between a data exporter who is a data controller and a data importer who acts as a data processor.

The Model Contracts require the data importer to process the personal data in accordance with certain mandatory EU data protection principles.

### US – EU Data Privacy Shield

For guidance, refer to the following ICO Guidance [that will be updated]:  

---


<table>
<thead>
<tr>
<th><strong>Binding Corporate Rules</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding Corporate Rules are effectively a global code of practice based on European data protection standards which once approved by relevant data protection authorities allow an international organisation to transfer personal data outside the EEA to its other group companies. Standard Contractual Clauses and Binding Corporate Rules can be used. More detail can be found in relevant ICO guidance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Consent</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The ICO will provide further guidance on this.</td>
</tr>
</tbody>
</table>
Annex 5: Access to personal data

A data subject has the same rights to access PV data as any other personal data as outlined below. Sample wording in response to a subject access request is set out in bold and italics below. The sample wording are just examples and should always be modified to take into account the particular circumstances and after having taken legal advice where necessary.

To know whether a company is processing personal data of which that person is the data subject.

Be given a description of the personal data, e.g.

*Data is held on patients who have experienced adverse events to enable us to understand more about the risks and benefits of a given product.*

Be told the purposes for which a company is processing their personal data, e.g.

*The information you provide will be used for the purpose of drug safety surveillance (and to enable us to deal with your enquiry appropriately).*

Be told whether the personal data will be given to any other company irrespective of location. This could include companies within the same group, partners, vendors, medicines regulatory authorities.

Be told the source of the personal data e.g.

*A report from a healthcare professional or information found through a review of a non-company sponsored website or, information received through a market research interview.*

A person has a right to the information constituting their personal data, has a right to update it, though not a right to see or obtain a copy of the documents that include the personal data.