PIPA
Pharmaceutical Information & Pharmacovigilance Association

pvlegal

abpi
Bringing medicines to *life*

Guidance notes on UK data protection in post-marketing pharmacovigilance

February 2013

Guidance notes on UK data protection in post-marketing pharmacovigilance

ABPI Pharmacovigilance Expert Network

Pharmaceutical Information and Pharmacovigilance Association (PIPA)

pvlegal

Approval Status

Authors: The ABPI Pharmacovigilance Expert Network, PIPA and pvlegal

Version: 1.0

Date: 11 February 2013

Acknowledgements: We thank the many stakeholders from industry, regulators and professional organisations who provided feedback in response to our consultation on the 2013 revision of this guidance document.

Table of contents

1. Introduction

This guidance has been developed by the Association of the British Pharmaceutical Industry (ABPI) Pharmacovigilance Expert Network (PEN), together with the Pharmaceutical Information and Pharmacovigilance Association (PIPA) and pvlegal to help companies performing post marketing pharmacovigilance (PV) in the UK to meet their data protection obligations under the UK Data Protection Act 1998 (DPA).

This guidance has been developed in consultation with the Information Commissioner's Office (ICO). It 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)[1].

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)[2] 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 enforces DPA compliance and can enforce compliance through criminal prosecution, non-criminal enforcement, audits and also has power to serve a monetary penalty notice on a company of up to £500,000 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.

1.2 Personal data in pharmacovigilance

Information is routinely collected by companies when carrying out PV to ensure the safety of patients and comply with regulatory obligations to report suspected adverse reactions to regulatory authorities[3]. 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 in order 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 Data Protection Directive states that whether or not an individual is identifiable depends on all the means likely to be reasonably used to identify them.

---

[1] The Data Protection Directive is currently being reviewed and a proposal for an EU Data Protection Regulation was published by the European Commission in January 2012. If adopted, the regulation will replace the Data Protection Directive and the DPA and will impact PV and many other life sciences company activities. It is unlikely to be adopted before 2014.

[2] The EEA consists of the EU Member States together with Iceland, Liechtenstein and Norway.

[3] Especially Directive 2001/83/CE November 6, 2001 Title IX.

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[4]. PV data relating to the health of a patient is generally considered sensitive personal data[5].

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

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

1.3 Scope

This guidance applies to PV data processed in the post marketing setting for which there is 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*)[6]. Activities performed as part of a clinical trial (under Volume 10)[7] 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[8].

2. Receipt of pharmacovigilance data and follow-up

2.1 Receipt of data

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*[9], 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 (eg a healthcare professional (HCP) or a patient's relative), it is not necessary to obtain consent from the

[4] 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

[5] Under the DPA, sensitive personal data are in some ways treated differently from other personal data. For example, the legal grounds under the DPA to process sensitive personal data are more limited and do not include when in the legitimate interests of the data controller. In addition, appropriate security measures (see Section 6 of this guidance) that need to be put in place are higher when processing sensitive personal data.

[6] European Medicines agency 2013. Good pharmacovigilance practices. Available at: http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/document_listing/document_listing_000345.jsp

[7] European Commission 2013. EudraLex - Volume 10 Clinical trials guidelines. Available at: http://ec.europa.eu/health/documents/eudralex/vol-10/

[8] 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

[9] http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2012/06/WC500129135.pdf

data subject in order to process personal data relating to the data subject for the purposes of PV[10]. 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 (eg 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.

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:

We advise that all patients are informed if an adverse event has been reported that relates to them.

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 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.

[10] In order to process personal data, a company must meet one of the conditions in schedule 2 of the DPA and in order to process sensitive personal data a company must also meet one of the conditions in schedule 3 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).

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.

At the time of writing, the European Commission considers a small number of countries outside the EEA to have adequate data protection laws[11].

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[12].

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[13] (see Annex 5).

4.2 Responding to a data subject access request

In the UK, access needs to be requested in writing (email is acceptable) and may be subject to a maximum £10 fee although companies are under no obligation to charge.

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 many 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.

[11] European Commission 2013. Commission decisions on the adequacy of the protection of personal data in third countries. Available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

[12] Information Commissioner's Office 2013. Anonymisation: managing data protection risk code of practice. Available at: www.ico.gov.uk/for_organisations/data_protection/topic_guides/anonymisation.aspx

[13] Legislation.gov.uk 1998. Data Protection Act 1998. Available at: www.legislation.gov.uk/ukpga/1998/29/section/7

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

Companies have 40 days to respond to a request from the date of receipt. If a fee is charged and/or more information is required from the requestor to identity the data subject or the location of the personal data, the 40 day period starts to run from the date on which both the fee (if one is applied) and the additional information has been received.

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[14]. 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.

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[15]. 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.

Companies must respond to an individual who has made a request to cease processing within 21 days of receiving the request. The response must explain why the company will be continuing to process some or all of the personal data relating to the individual eg

The 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' ie 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.

[14] Official Journal of the European Union 2012. Commission implementing regulation (EU) No 520/2012 of 19 June 2012 on the performance of pharmacovigilance activities provided for in Regulation (EC) No 726/2004 of the European Parliament and of the Council and Directive 2001/83/EC of the European Parliament and of the Council. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:159:0005:0025:EN:PDF

[15] Legislation.gov.uk 1998. Data Protection Act 1998. Available at: www.legislation.gov.uk/ukpga/1998/29/section/10

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, 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 eg 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 on 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[16].

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[17].

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

[16] Official Journal of the European Union 2012. Commission implementing regulation (EU) No 520/2012 of 19 June 2012 on the performance of pharmacovigilance activities provided for in Regulation (EC) No 726/2004 of the European Parliament and of the Council and Directive 2001/83/EC of the European Parliament and of the Council. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:159:0005:0025:EN:PDF

[17] Legislation.gov.uk 1998. Data Protection Act 1998. Available at: www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/II/crossheading/the-seventh-principle

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[18].

Notification should be made using the standard notification form available at 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 eg:

Collecting, 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.

[18] Information Commissioner's Office 2013. Register of data controllers. Available at: www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

Annex 1: Abbreviations

Abbreviation	
AE	Adverse Event
AOR	Acknowledgement of Receipt
BCR	Binding Corporate Rules
DPA	UK Data Protection Act
DPN	Data Protection Notice
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EMA	European Medicines Agency
EU	European Union
HCP	HealthCare Professional
ICO	Information Commissioner's Office
ICSR	Individual Case Safety Report
MA	Marketing Authorisation
MAH	Marketing Authorisation Holder
MHRA	Medicines and Healthcare products Regulatory Agency
PEN	ABPI Pharmacovigilance Expert Network
PIPA	Pharmaceutical Information and Pharmacovigilance Association
PV	Pharmacovigilance
UK	United Kingdom
WP	Working Party

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

Term	Meaning
Data	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 (eg 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.
Data Controller	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.
Data Processor	Any person, other than the data controller's employees, who processes personal data on behalf of the data controller.
Data Subject	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.
Personal Data	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.
Sensitive Personal Data	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.
Processing	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.
Relevant Filing System	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.

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:

> ***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[19]. You have a right of access to your personal data which we hold about you.***

[19] 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

Face to face (ie 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.

Enquiries/report for non-company products

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

Follow-up of pharmacovigilance data

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:

> ***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. The ICO recommends a good practice approach as follows[20] (see table below for further details – in sequential order):

- **Step 1:** will personal data be transferred to a third country?
- **Step 2:** do the third country and circumstances surrounding the transfer ensure an adequate level of protection?
- **Step 3:** can adequate safeguards be put in place?
- **Step 4:** do any other derogations in the DPA 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'.

The adequacy test involves assessing all the circumstances of the case, including the nature of the personal data to be transferred, the purposes of the proposed transfer, the period during which the data are intended to be processed and any security measures taken in respect of the data. In addition, companies should consider the law in force in the third country, the international obligations of the third country and any codes of conduct enforceable in that country (the 'Legal Adequacy Criteria'). However, as sensitive personal data is likely to be processed as part of PV, consideration should be given to use of the other data transfer solutions referred to below.

The adequacy assessment is also likely not to be accepted in other EU Member States as a basis for the transfer of personal data from the EEA under the data protection laws in those EU Member States.

Model Contracts[21]

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[22] and

(ii) transfers between a data exporter who is a data controller and a data importer who acts as a data processor[23].

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

[20] Information Commissioner's Office 2008. *The eighth data protection principle and international data transfers.* Available at: www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/international_transfers_legal_guidance_v2.0_300606.pdf

[21] European Commission 2013. *Model Contracts for the transfer of personal data to third countries.* Available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm#h2-5

[22] Official Journal of the European Union 2001. *Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (2001/497/EC) and Commission Decision of 27 December.* Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF

[23] Official Journal of the European Union 2010. *Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.* Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF

US Safe Harbor

Transfer to US companies listed by the US Department of Commerce as subscribing to the principles of the Safe Harbor privacy framework which exists for transfers of Personal Data from the EEA and from Switzerland. Safe Harbor involves annual self-certification under which registrants are required to comply with a set of Safe Harbor principles and to put in place comprehensive internal data protection policies and procedures with adequate levels of data protection. US Safe Harbor is enforced by the US Federal Trade Commission[24].

Binding Corporate Rules

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[25].

Consent

The ICO in its guidance on data transfers has commented that consent is unlikely to provide an adequate long-term framework in cases of repeated or structural transfers of personal data to a third country as consent to be valid must give the individual a real opportunity to withhold consent. The EU Article 29 Working Party[26] has also stated that consent is not an appropriate basis for systematic international personal data transfers. Moreover, in PV, reliance on consent is likely to be difficult because companies do not necessarily have contact with all data subjects.

The problems with consent have caused the Working Party to comment that consent is unlikely to provide an adequate long-term framework for companies in cases of repeated or even structural transfers for the processing in question "particularly if the transfer forms an intrinsic part of the main processing (eg centralisation of a world database, which needs to be fed by continual and systematic data transfers to be operational)"[27].

According to the Working Party, companies could find themselves in insoluble situations if just one data subject subsequently decided to withdraw his consent. Relying on consent may therefore prove to be a 'false good solution', simple at first but in reality complex and cumbersome.

[24] Export.gov 2013. *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*. Available at: http://export.gov/safeharbor/index.asp

[25] Information Commissioner's Office 2008. *Binding corporate rules*. Available at: http://www.ico.gov.uk/for_organisations/data_protection/overseas/binding_corporate_rules.aspx

[26] European Commission 2012. *Article 29 Working Party*. Available at: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

[27] European Commission 2007. *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 adopted on 25 November 2007 – WP 114*. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf

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 purple 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, eg

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, eg

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 eg

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 and not a right to see or have a copy of the documents that include the personal data.

Association of the British Pharmaceutical Industry
7th Floor, Southside, 105 Victoria Street, London SW1E 6QT
t +44 (0)870 890 4333 abpiregulatory@abpi.org.uk
www.abpi.org.uk