Picker

Data Protection and Processing Policy

Version: 1.3 External

Date: July 2023

Contents

1. Introduction

The Picker Group, comprising Picker Institute Europe and Picker HWA (the “Group”) uses personal information about people with whom it deals in order to carry out its activities and provide its services. Such people include patients, service users, family members, employees (past, present and prospective), clients, suppliers and other business contacts. The information includes name, address, email address, data of birth, private and confidential information and more sensitive information (referred to as **special category personal data**), such as information relating to health or racial origin.

The lawful and proper treatment of **personal data** by the Group is extremely important to the success of our organisation in order to maintain the confidence of our business partners and clients. Aside from the potential damage to the Group's reputation and goodwill, breaches of **data protection laws** can lead to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover (whichever is higher), legal claims from affected individuals and potential criminal proceedings.

All of the Group’s staff are all responsible for ensuring that the Group conducts its operations to the highest standards in accordance with the privacy principles of the UK GDPR. It is an integral part of our service offering to **process client personal data** which we must do in accordance with **data protection law**.

This Data Protection and Processing Policy sets out how we process **client personal data** in order to meet these requirements and applies to all **of the Group’s staff** who are involved in the **processing** of or have access to **client personal data** including all the Group’s employees, contractors, Board of Trustees, temporary staff, freelancers, secondees and volunteers.

Should you have any comments or questions in relation to any of the matters referred to in this Data Protection and Processing Policy they should be referred in the first instance to the Group’s Data Protection Officer (**DPO**) who is currently Mike Donoghue, DPO@pickereurope.ac.uk

2. Key terms

It is important to note that **personal data** includes (but is not limited to):

- contact information provided by the client for survey respondents such as their names and addresses;
- survey response data if it specifically refers to or names identifiable individuals such as in free text comments;
- data inputted onto our systems from survey responses for so long as we have the ability to identify the respondents from other data we hold;
- contact information submitted via Picker.org;
- contact information for our clients, business partners and other contacts relating to our business; and
- internal information relating to the Group’s Staff.

Additional information concerning the meaning of the words and expressions which are in bold in this Data Protection and Processing Policy are set out in the glossary at the end of this document.

3. Our role as a data processor and data controller

We act as a **data processor** for our clients and in doing so we must ensure that we:

i. only use **client personal data** for the specific purposes and in the specific manner agreed with the client; and

ii. do not extract, re-utilise, use, exploit, redistribute, re-disseminate, copy or store **client personal data** other than for the purposes of providing our services and in accordance with our standard operating procedures and client contracts.

We are also responsible for:

- ensuring that we are able to demonstrate our compliance with our obligations under **data protection laws**; and
- the activities of our subcontractors such as printing or mailing house, data capture, transcribing, language translator, computer assisted telephone interviews and for ensuring that they comply with these requirements.

As part of these requirements, we must ensure that any instructions received from clients to **process personal data** otherwise than in accordance with the terms of the client contract are confirmed in writing by the client before being acted upon and that any instructions to our subcontractors are also given in writing.

Aside from acting as **data processor** for our clients, we are also the **data controller** for any **personal data** which we collect and process for our own purposes. That personal data includes information we hold about contacts at our clients and business partners as well as internal information concerning the Group's Staff.

The terms of this policy, unless specifically referenced to **survey respondent personal data**, apply to the processing of all **personal data** whether it is **client personal data** or any other **personal data** we hold.

4. Data transfer and storage

It is a fundamental principle of data protection that **personal data** is kept secure and the Group has developed policies and procedures for ensuring that this is the case at all times.

In dealing with any **survey respondent personal data,** the Group staff are required to follow the following policies and procedures whereby:

- all survey respondent personal data which we received from a client, such as survey respondent names, addresses and other details, is transferred to us via a secure file transfer web portal using the HTTPS protocol whereby all users access to the intended data is further protected by username and password authentication

- all survey respondent personal data must be correctly transferred and stored in accordance with our Quality Assurance and Information Security Management Systems.
- whenever possible personal identifiers are removed from data being processed (which is known as "pseudonymisation" under **data protection laws)** and in particular that:
    - a unique reference number or barcode etc is created and linked to each data subject which is then used for internal purposes (such as tracking who responds and who to send reminders to for the relevant survey);
    - in inputting survey respondent data, any references to individuals or from which individuals could be identified in free text comments (such as references to staff, patients, service users, unit, ward, etc.) must be replaced by pseudo blanks such as ****** (or similar) or otherwise removed, unless specified otherwise;
- all **survey respondent personal data** for each survey or other project is at all times securely stored with restricted access to the files/folders as relevant ;
- **survey respondent personal data** is kept no longer than is strictly necessary (this is usually a maixum of six months unless agreed otherwise with a client) for us to perform our obligations to the client and for example survey respondent names and addresses are deleted from our systems as soon as we have no further use of them; and
- access to **survey respondent personal data** is limited to only **the Group's staff** who need access in order to perform our services (including internal audit).

These procedures are required to enable us to comply with our obligations under **data protection laws** as well as our contractual obligations to our clients and must be strictly adhered to.

We must also ensure that our subcontractors adopt similar procedures and, in particular, that they confirm to us and/or we check with them that **personal data** is deleted once it is no longer required.

5. Processing of personal data belonging to minors (children under the age of 13)

Some projects include the processing of **personal data** belonging to minors (children under the age of 13). Any processing of such data should follow the same guidance as all **personal data**. Parental consent should be sought, and evidenced. This may not be necessary if the **personal data** has been shared via a **Section 251** approval process.

6. Retention of data

As noted above **client personal data** should only be retained for as long as is necessary for us to perform our obligations to our client and must be securely destroyed or deleted from our systems once it is no longer needed at the written request of the Client or after 6 months of the project closing or under the applicable client agreement.

However, anonymised data (which is not classed as personal data) may be held for longer purposes provided that all information that might link the survey respondent with the data has been removed from our systems and, for example, it is not possible for us to identify a survey respondent from their reference number.

Other **personal data** can be kept for longer but must be kept under review, abiding by applicable policies (eg the Picker Group Staff Privacy Policy) and deleted when it is no longer required.

7. Deletion of data

Deletion of **personal data** must be carried out in accordance with our Quality Assurance and Information Security Management Systems.

8. Rectification and removal of data

We must ensure that all **personal data** we hold is accurate and, where necessary, kept up to date. Therefore, if we are notified at any time by either a client or a **data subject** that **client personal data** is in any way inaccurate, such as a survey respondent's name or address, it must be corrected without delay when inaccurate.

Moreover, data subjects have a right to object to the **processing** of their **personal data** by our clients or by us on their behalf**.** Accordingly, if we are instructed to cease **processing** an individual's data by our client we must do so immediately. If such a request is received from a data subject directly then it must be referred to the DPO and then follow the DPO's directions to refer it on to the client.

Further guidance on requests from **data subjects** can be found in **the Data Subject Access Request policy.**

9. Subcontractors

As a **data processor** and **data controller** we are under a legal obligation under **data protection laws** to ensure that our subcontractors comply with the same obligations as we undertake to our clients to the extent that they assist us with processing **personal data**.

All of our subcontractors have been carefully selected to ensure that they meet the same high standards as we do and have contractually committed to the Group to meet the same standards and requirements as the Group undertakes to its clients.

10. Privacy statements

Our privacy statements can be accessed through our website or are available from the DPO.

For surveys conducted via our web portal, a separate privacy statement applies which names the applicable client as the controller of the **survey respondent personal data** submitted via the portal.

In addition, for certain projects we may be asked by the client to include a form of privacy statement to be issued with the survey materials.

If this is the case, the client will inform us and will provide the form of privacy statement to be used. As a data processor, our role is to ensure that these privacy statements are included in the survey materials sent to the survey respondents.

11. IT security arrangements

Data protection laws require that **personal data** is kept secure by appropriate technical and organisational measures against unauthorised or unlawful **processing**, and against accidental loss, destruction or damage.

In order to comply with this obligation, the Group has developed systems and safeguards to ensure that client personal data is kept secure including through the use of encryption and survey respondent reference numbers where applicable. Furthermore, in order to meet the technical requirements of **data protection laws** the Group's IT systems have been assessed to meet the best practice specifications for an information security management system set down by the ISO 27001 standard.

As part of the Group's security arrangements all Picker staff are required to adhere to our IT and Security Policy in relation to the use of personal devices, such as mobile phones, to ensure that our data security procedures are not compromised in any way.

12. Reporting a personal data breach

Personal data breaches arise in any situation where the confidentiality or integrity of **personal data** is compromised. This might occur for reasons such as, but not limited to:

- Unauthorised access to our systems;
- Loss of data including any loss of any device which may contain or allow access to **personal data** (e.g. the loss of any laptop, mobile phone, external hard drive, usb stick etc);
- **Personal data** being sent by email; or
- The mis-posting of information relating to a survey respondent.

If such an event happens we must deal with it in an open, transparent and professional manner to ensure that any threat or risk to the data subject's and/or our client's interests is kept to a minimum.

In particular any breach (suspected or otherwise) must be reported to the DPO as soon as possible particularly, as under the terms of our agreements with our clients, we are required to notify any **personal data breach** to them as soon as we become aware of it. It should also be borne in mind that we are responsible for any **personal data breach** of our subcontractors if it relates to **personal data**.

As a consequence, if Group staff know or suspect that a **personal data breach** has occurred or is likely to occur, they must immediately contact the DPO and follow the DPO's directions in dealing with the data breach.

13. Transfers of personal data

Personal data must only be transferred either to our client or to our authorised subcontractors to the extent they need it to provide their services.

Under the terms of our agreements with our clients we are also restricted from transferring **client personal data** to countries outside the UK or EEA without prior agreement. Where we use suppliers (such as software as a service) who may have facilities outside of the UK or EEA, the DPO will be responsible for ensuring the correct documentation is in place.

14. Data subject's rights and requests

Data subjects, including the Group's employees and contractors, have rights in connection with the processing of their **personal data** including rights to:

- withdraw consent to **processing** at any time;
- receive certain information about the data controller's **processing** activities;
- request access to their **personal data** that the **data controller** holds;
- receive access to their **personal data** free of charge, unless a request is deemed excessive, under which circumstances the Group reserve the right to charge a nominal fee;
- to typically have their request actioned within one month, under normal circumstances;
- prevent our use of their **personal data** for direct marketing purposes;
- ask the data controller to erase **personal data** if it is no longer necessary in relation to the purposes for which it was collected or **process**ed or to rectify inaccurate data or to complete incomplete data;
- restrict **processing** in specific circumstances;
- challenge **processing** which has been justified on the basis of the data controller's legitimate interests or in the public interest;
- request a copy of any agreement under which **personal data** is transferred outside of the UK/EEA;
- object to decisions based solely on automated **processing**, including profiling;
- prevent **processing** that is likely to cause damage or distress to the **data subject** or anyone else;
- be notified of a **personal data breach** which is likely to result in high risk to their rights and freedoms;
- make a complaint to the Group or to the Information Commissioner's Office; and
- in limited circumstances, receive or ask for their **personal data** to be transferred to a third party in a structured, commonly used and machine readable format.

Any such request will usually be made to our client as the **data controller** in the first instance although we must assist the client in responding to any such request and comply with any directions made by our client as a consequence of the request. Further information on data subject requests, including how to process a request and further details on the rights listed above, is included in the Picker Data Subject Access Requests Policy.

If we receive such a request directly from a survey respondent, the DPO will respond to any such request.

15. Privacy and Electronic Communication Regulations (PECR)

Picker are required to comply with the Privacy and Electronic Communications Regulations and will review our compliance obligations on at least an annual basis. Our staff are responsible for complying with all processes, including but not limited to the IT User Agreement, to help Picker meet our compliance obligations.

16. Changes to this Data Protection and Processing Policy

This Data Protection and Processing Policy will be kept under review. The version found on the Picker website should be regarded as the most current.

Glossary

client personal data: survey respondent personal data and contact details of individuals at our clients.

data controller: a person or organisation that determines the purpose and the means as to when, why and how to **process personal data**. For all **survey respondent personal data** this will be our client.

data processor: a person or organisation that processes personal data on the instructions or on behalf of a data controller.

data subject: a living, identified or identifiable individual about whom we hold **personal data**. **Data subjects** may be nationals or residents of any country and may have legal rights regarding their **personal data**. All survey respondents will be **data subjects**.

data protection laws: means all applicable laws in the UK in relation to the protection and processing of personal data including the UK General Data Protection Regulation and the Data Protection Act 2018.

personal data: any information identifying a **data subject** or information relating to a **data subject** that we can identify (directly or indirectly) from that data alone or in combination with other information we possess or can reasonably access. This would include therefore any information about survey respondents where we hold information separately which allows us to identify the relevant individuals. It also includes contact information we hold about our clients and business partners and information concerning the Group's Staff. **Personal data** includes **special category personal data.** Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

personal data breach: any act or omission that compromises the security, confidentiality or integrity of **personal data** or the physical, technical, administrative or organisational safeguards that we or our third party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of **personal data** is a **personal data breach**.

The Group's staff: all officers, employees, contractors, temporary staff, freelancers, secondees and volunteers of the Picker Group

processing or **process**: any activity that involves the use of or access to **personal data**. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. **Processing** also includes transmitting or transferring **personal data** to third parties.

Section 251: Section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidence for defined medical purposes, such as healthcare research.

special category personal data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and **personal data** relating to criminal offences and convictions.

survey respondent personal data: the names, addresses and other contact details of survey respondents and any personal data provided to us by survey respondents for so long as they or individuals referred to in it can be identified from it or other information that we hold.