onEvidence Ltd. Cotton Court, Preston PR1 3BY Company #12668322

Data Protection Policy

(IGP-2)

Summary			
This Policy sets out how onEvidence (the Business) processes the personal data that it holds (relating to staff, research participants and third parties). It outlines the Business' responsibilities under data protection legislation and regulation, setting out how it will comply, and provides instruction for staff handling personal data.			
Scope			
The Policy applies to all staff employed by onEvidence (the Business), including contractors who are carrying out work on behalf of the business.			
Document control			
Document type	Information Governance Policy – IGP-2		
Document owner	Board of Directors		
Lead contact	Dr Roxanne Khan		
Document status	Approved		
Version	V.1		
Approved by	Board	Date	14 April 2023
Date of publication	April 2023	Next review date	April 2025
Date of original publication	April 2023	Review frequency	2 years
Superseded documents	N/A		
Related documents	See 'Interaction with other policies and procedures' below		

Contents

1. Introduction

The protection of individuals via the lawful, legitimate and responsible processing and use of their personal data is a fundamental human right. Individuals may have a varying degree of understanding or concern for the protection of their personal data, but the Business must respect their right to have control over their personal data and ensure it acts in full compliance with legislative and regulatory requirements at all times.

The General Data Protection Regulation (GDPR), as supplemented by the Data Protection Act 2018 (DPA), is the main piece of legislation that governs how the Business collects and processes personal data.

2. Purpose of this policy

This Policy sets out how the Business will process the personal data of its staff, research participants, suppliers and other third parties. This Policy applies to all personal data that the Business processes regardless of the format or media on which the data are stored or who it relates to.

A glossary of the terms used throughout the Policy can be found in Appendix 1.

3. Scope of this Policy

This Policy applies to all staff of the Business and any individual carrying out work on behalf of the Business (referred to herein as you/your) involving the handling personal data.

Compliance with this Policy and the related policies and procedures set out in Appendix 2 is mandatory. Any breach of this Policy and any related policies and procedures may result in disciplinary action.

Dr Roxanne Khan is responsible for overseeing the implementation and review of this Policy (and the related policies and procedures). They can be contacted as follows:

rkhan@onevidence.co.uk | Telephone: 01772 348316

4. Data protection principles

The GDPR is based on a set of core principles that the Business must observe and comply with at all times from the moment that personal data are collected until the moment that personal data are archived, deleted or destroyed.

The Business must ensure that all personal data are:

a) Processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency).
b) Collected only for specified, explicit and legitimate purposes
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed
d) Accurate and where necessary kept up to date
e) Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed
f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

Additionally, the Business must ensure that:

a) Personal data are not transferred outside of the EEA (which includes the use of any website or application that is hosted on servers located outside of EEA) to another country without appropriate safeguards being in place
b) The Business allows data subjects to exercise their rights in relation to their personal data
c) The Business is responsible for, and must be able to demonstrate compliance with, all of the above principles.

5. Lawfulness, fairness and transparency

Lawfulness and fairness

In order to collect and process personal data for any specific purpose, the Business must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal data has been collected, consulted, used or otherwise processed by the Business.

Processing personal data will only be lawful where at least one of the following lawful bases applies:

a) The data subject has given their consent for one or more specific purposes
b) The processing is necessary for the performance of a contract to which the data subject is a party (for instance a contract of employment with the Business)
c) To comply with the Business' legal obligations
d) To protect the vital interests of the data subject or another person (this will equate to a situation where the processing is necessary to protect the individual's life)

e) To perform tasks carried out in the public interest or the exercise of official authority (generally research in the Business' case)
f) To pursue the Business' legitimate interests where those interests are not outweighed by the interests and rights of data subjects (only available to the Business in some circumstances)
g) The Business must identify and document the lawful basis relied upon by it in relation to the processing of personal data for each specific purpose or group of related purposes.

Consent as a lawful basis for processing

There is no hierarchy between the lawful bases for processing above, of which a data subject's consent is only one. Consent may not be the most appropriate lawful basis depending on the circumstances.

In order for a data subject's consent to be valid and provide a lawful basis for processing, it must be:

- specific (not given in respect of multiple unrelated purposes)
- informed (explained in accessible and plain language)
- unambiguous and given by a clear affirmative action (meaning opt-in: silence or inactivity will not be sufficient)
- separate and unbundled from any other terms and conditions provided to the data subject
- freely and genuinely given (there must not be any imbalance in the relationship between the Business and the data subject and consent must not be a condition for the provision of any service or product)

A data subject must be able to withdraw their consent as easily as they gave it. Once consent has been given, it will need to be updated where the Business wishes to process the personal data for a new purpose that is not compatible with the original purpose for which they were collected.

Unless the Business is able to rely on another lawful basis for processing, a higher standard of explicit consent (where there can be no doubt that consent has been obtained, for example a signed document or a Yes/No option accompanied by clear consent wording) will usually be required to process special categories of personal data (see glossary for definition), for automated decision-making and for transferring personal data outside of the EEA.

Where the Business needs to process special categories of personal data, it will generally rely on another lawful basis that does not require explicit consent; however, the Business must provide the data subject with a fair processing notice explaining such processing.

If the Business is unable to demonstrate that it has obtained consent in accordance with the above requirements, it will not be able to rely upon such consent.

Transparency

The concept of transparency runs throughout the GDPR and requires the Business to ensure that any information provided by the Business to data subjects about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language. Where the Business has not been transparent about how it processes personal data, this will call the lawfulness and fairness of the processing into question.

The Business can demonstrate transparency through providing data subjects with appropriate privacy notices or fair processing notices before it collects and processes their personal data and at appropriate times throughout the processing of their personal data.

The GDPR sets out a detailed list of information that must be contained in all privacy notices and fair processing notices, including the types of personal data collected; the purposes for which they will be processed; the lawful basis relied upon for such processing (in the case of legitimate interests, the Business must explain what those interests are); the period for which they will be retained; who the Business may share the personal data with; and, if the Business intends to transfer personal data outside of the EEA, the mechanism relied upon for such transfer (see Transfers of personal data outside of the EEA).

Where the Business obtains any personal data about a data subject from a third party (for example, CVs from recruitment agents for potential employees) it must check that it was collected by the third party in accordance with the GDPR's requirements and on a lawful basis where the sharing of the personal data with the Business was clearly explained to the data subject.

All privacy notices and fair processing notices should be reviewed by the Board of Directors (rkhan@onevidence.co.uk).

6. Purpose limitation

The Business must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to data subjects before the personal data have been collected.

The Business must ensure that it does not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. Where the Business intends to do so, it must inform the data subjects before using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

7. Data minimisation

The Business must handle personal data in a manner that ensures data protection by design and default. Data minimisation is an important element of this and can include pseudonymisation of personal data (partial anonymisation), limiting what information is held, restricted access, sharing and retention.

The personal data that the Business collects, and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

You must only process personal data when necessary for the performance of your duties and tasks and not for any other purposes. Accessing personal data that you are not authorised to access, or that you have no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

You may only collect personal data as required for the performance of your duties and tasks and should not ask a data subject to provide more personal data than is strictly necessary for the intended purposes.

You must ensure that when personal data are no longer needed for the specific purposes for which they were collected, that such personal data are deleted, destroyed or anonymised.

8. Accuracy

The personal data that the Business collects and processes must be accurate and, where necessary, kept up-to-date and must be corrected or deleted without delay when the Business discovers, or is notified, that the data are inaccurate.

You must ensure that you update all relevant records if you become aware that any personal data are inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.

9. Storage limitation

The personal data that the Business collects and processes must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected (except in order to comply with any legal, accounting or reporting requirements).

Storing personal data for longer than necessary may increase the severity of a data breach and may also lead to increased costs associated with such storage.

The Business will maintain policies and procedures to ensure that personal data are deleted, destroyed or anonymised after a reasonable period of time following expiry of the purposes for which they were collected.

You must regularly review any personal data processed by you in the performance of your duties and tasks to assess whether the purposes for which the data were collected have expired. Where appropriate, you must take all reasonable steps to delete or destroy any personal data that the Business no longer requires.

All privacy notices and fair processing notices must inform data subjects of the period for which their personal data will be stored or how such period will be determined.

10. Security, integrity and confidentiality

Security of personal data

The personal data that the Business collects and processes must be secured by appropriate technical and organisational measures against loss, destruction or damage, and against unauthorised or unlawful processing.

The Business will develop, implement and maintain appropriate technical and organisational measures for the processing of personal data taking into account the:

- nature, scope, context and purposes for such processing
- volume of personal data processed
- likelihood and severity of the risks of such processing for the rights of data subjects

The Business will regularly evaluate and test the effectiveness of such measures to ensure that they are adequate and effective.

You are responsible for ensuring the security of the personal data processed by you in the performance of your duties and tasks.

You must ensure that you follow all procedures that the Business has put in place to maintain the security of personal data from collection to destruction.

You must ensure that the confidentiality, integrity and availability of personal data are maintained at all times:

- **Confidentiality**: means that only people who need to know and are authorised to process any personal data can access it
- **Integrity**: means that personal data must be accurate and suitable for the intended purposes
- **Availability**: means that those who need to access the personal data for authorised purposes are able to do so

You must not attempt to circumvent any administrative, physical or technical measures the Business has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

Reporting personal data breaches

In certain circumstances, the GDPR will require the Business to notify the ICO, and potentially data subjects, of any personal data breach.

The Business has put in place appropriate procedures to deal with any personal data breach and will notify the ICO and/or data subjects where the Business is legally required to do so.

If you know or suspect that a personal data breach has occurred, you must contact Dr Roxanne Khan immediately to report it and obtain advice and take all appropriate steps to preserve evidence relating to the breach.

11. Sharing personal data

You are not permitted to share personal data with third parties unless the Business has agreed to this in advance, this has been communicated to the data subject in a privacy notice or fair processing notice beforehand and, where such third party is processing the personal data on our behalf, the Business has undertaken appropriate due diligence of such processor and entered into an agreement with the processor that complies with the GDPR's requirements for such agreements.

The transfer of any personal data to an unauthorised third party would constitute a breach of the Lawfulness, fairness and transparency principle and, where caused by a security breach, would constitute a personal data breach. Do not share any personal data with third parties, including the use of freely available online and cloud services for work-related purposes, unless you are certain that the conditions outlined above apply. Seek advice from Dr Roxanne Khan if you are unsure.

12. Transfers outside of the European Economic Area

The GDPR prohibits the transfer of personal data outside of the EEA in most circumstances in order to ensure that personal data are not transferred to a country that does not provide the same level of protection for the rights of data subjects. In this context, a "transfer" of personal data includes transmitting, sending, viewing or accessing personal data in or to a different country.

The Business may only transfer personal data outside of the EEA if one of the following conditions applies:

- the European Commission has issued an "adequacy decision" confirming that the country to which we propose transferring the personal data ensures an adequate level of protection for the rights and freedoms of data subjects (this applies to only a small number of countries)
- appropriate safeguards are in place, such as binding corporate rules, standard contractual clauses that have been approved by the European Commission, an approved code of

conduct or certification mechanism which, in each case, can be obtained from the Information Governance Manager and Data Protection Officer

- the data subject has given their explicit consent to the proposed transfer, having been fully informed of any potential risks
- the transfer is necessary in order to perform a contract between the Business and a data subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject in circumstances where the data subject is incapable of giving consent
- the transfer is necessary, in limited circumstances, for the Business' legitimate interests

You must ensure that you do not transfer any personal data outside of the EEA except in the circumstances set out above and provided that the Business has agreed to this in advance.

13. Data subject rights and requests

The GDPR provides data subjects with a number of rights in relation to their personal data. These include:

- **Right to withdraw consent**: where the lawful basis relied upon by the Business is the data subject's consent, the right to withdraw such consent at any time without having to explain why
- **Right to be informed**: the right to be provided with certain information about how we collect and process the data subject's personal data (see Transparency)
- **Right of subject access**: the right to receive a copy of the personal data that we hold, including certain information about how the Business has processed the data subject's personal data
- **Right to rectification**: the right to have inaccurate personal data corrected or incomplete data completed
- **Right to erasure (right to be forgotten)**: the right to ask the Business to delete or destroy the data subject's personal data if: the personal data are no longer necessary in relation to the purposes for which they were collected; the data subject has withdrawn their consent (where relevant); the data subject has objected to the processing; the processing was unlawful; the personal data have to be deleted to comply with a legal obligation; the personal data were collected from a data subject under the age of 13, and they have reached the age of 13
- **Right to restrict processing**: the right to ask the Business to restrict processing if: the data subject believes the personal data are inaccurate; the processing was unlawful and the data subject prefers restriction of processing over erasure; the personal data are no longer necessary in relation to the purposes for which they were collected but they are required to establish, exercise or defend a legal claim; the data subject has objected to the processing pending confirmation of whether the Business' legitimate interests grounds for processing override those of the data subject

- **Right to data portability**: in limited circumstances, the right to receive or ask the Business to transfer to a third party, a copy of the data subject's personal data in a structured, commonly-used machine-readable format
- **Right to object**: the right to object to processing where the lawful basis for processing communicated to the data subject was the Business' legitimate interests and the data subject contests those interests
- **Right to object to direct marketing**: the right to request that we do not process the data subject's personal data for direct marketing purposes
- **Right to object to decisions based solely on automated processing (including profiling)**: the right to object to decisions creating legal effects or significantly affecting the data subject which were made solely by automated means, including profiling, and the right to request human intervention
- **Right to be notified of a personal data breach**: the right to be notified of a personal data breach which is likely to result in a high risk to the data subject's rights or freedoms
- **Right to complain**: the right to make a complaint to the ICO or another appropriate supervisory authority

You must be able to identify when a request has been made and must verify the identity of the individual making a request before complying with it. You should be wary of third parties deceiving you into providing personal data relating to a data subject without their authorisation.

You must immediately forward any request made by a data subject (even if you are uncertain whether it represents a request as set out above) to Dr Roxanne Khan. The Business will only have 30 days to respond in most circumstances.

14. Research exemption

Some of the rules outlined above do not apply when personal data is being used for research purposes due to an exemption contained in the GDPR and DPA 2018. This exemption applies if the following conditions are met:

a) Appropriate technical and organisational safeguards exist to protect the personal data e.g. data minimisation, pseudonymisation, or access controls.
b) There is no likelihood of substantial damage or distress to the data subjects from the data processing.
c) The research will not lead to measures or decisions being taken about individuals (except for ethically approved interventional medical purposes).
d) Compliance with the requirements that the exemption negates would prevent or seriously impair the research purpose.

If these conditions apply, then the following rules can be applied:

a) Personal data originally collected for other purposes can be used for the research and can be kept indefinitely.

b) The right of individuals to access their personal data does not apply if the research results will be made public in a form that does not identify them.
c) The rights of rectification, erasure, restriction and objection do not apply.

15. Accountability and record-keeping

The Business is responsible for and must be able to demonstrate compliance with the data protection principles and the Business' other obligations under the GDPR. This is known as the 'accountability principle'.

The Business must ensure that it has adequate resources, systems and processes in place to demonstrate compliance with the Business' obligations including:

- appointing a suitably experienced Data Protection Officer (DPO) and providing them with adequate support and resources
- ensuring that at the time of deciding how the Business will process personal data, and throughout its processing, implementing appropriate technical and organisational measures that are designed to ensure compliance with the data protection principles (known as 'Data Protection by Design')
- ensuring that, by default, only personal data that are necessary for each specific purpose are processed both in relation to the nature, extent and volume of such personal data, the period of storage and the accessibility of the personal data (known as 'Data Protection by Default')
- ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, the Business has carried out an assessment of those risks and is taking steps to mitigate those risks, by undertaking a 'Data Protection Impact Assessment' (see below)
- integrating data protection into the Business' internal documents, privacy policies and fair processing notices
- regularly training the Business' staff on the GDPR, this Policy and the Business' related policies and procedures
- regularly testing the measures implemented by the Business and conducting periodic reviews to assess the adequacy and effectiveness of this Policy, and the Business' related policies and procedures

The Business must keep full and accurate records of all its processing activities in accordance with the GDPR's requirements.

You must review all the systems and processes under your control to ensure that they are adequate and effective for the purposes of facilitating compliance with the Business' obligations under this Policy.

16. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data. DPIAs are required for processing likely to result in high risk to the individuals and their personal data, and where new technologies are involved. In practice, the Business requires a DPIA for any projects involving the use of personal data.

A DPIA must:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks.

DPIAs need to be assessed and signed off by Dr Roxanne Khan.

17. Direct marketing

In addition to the Business' obligations under the GDPR, it is also subject to more specific rules in relation to direct marketing by email, fax, SMS or telephone. The Business must ensure that it has appropriate consent from individuals to send them direct marketing communications, and that when a data subject exercises their right to object to direct marketing it has honoured such requests promptly.

You must ensure that you understand or consult with Dr Roxanne Khan on the Business' legal obligations in relation to direct marketing before embarking upon any direct marketing campaign.

Appendix 1: Glossary of terms

automated processing: any form of processing (including profiling) that is undertaken by automated means to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data about them

controller: the person or organisation that determines the purposes and means of processing personal data

criminal convictions and offences: personal data relating to criminal convictions, the commission or alleged commission of an offence, proceedings for the commission or alleged commission of an offence and sentencing

Data Protection Impact Assessment (DPIA): a tool used to identify and reduce the risks of a processing activity and which must be undertaken in certain circumstances specified in the GDPR

data subject: an individual to whom personal data relates and who can be identified or is identifiable from personal data

Data Protection Officer (DPO): a person required to be appointed in specific circumstances under the GDPR and who must have expert knowledge of data protection law and practice, being the organisation's main representative on data protection matters

DPA 2018: the UK Data Protection Act 2018

EEA: the 28 countries in the European Union and Iceland, Lichtenstein and Norway

explicit consent: a higher standard of consent that requires a very clear and specific statement rather than an action which is suggestive of consent

fair processing notices: a notice setting out information that must be provided to data subjects before collecting personal data from them, including notices aimed at a specific group of individuals or notices that are presented to a data subject on a 'just-in-time' basis (also known as 'privacy notice' or 'data protection notice')

GDPR: the General Data Protection Regulation (Regulation (EU) 2016/679)

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 identifiers we possess or can reasonably access. Personal data includes criminal convictions and

offences data, special categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. 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: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and which compromises the confidentiality, integrity, availability and/or security of the personal data

privacy notices: see fair processing notices above

process, processes, processing: any activity or set of activities which involves personal data including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment or combination, restriction, erasure or destruction

pseudonymised, pseudonymisation: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers (for example, a numerical identifier or other code) or pseudonyms so that the data subject cannot be identified without combining the identifier or pseudonym with other information which has been kept separately and securely. Personal data that have been pseudonymised is still treated as personal data (unlike personal data which has been anonymised)

special categories of personal data: previously known as “sensitive personal data” under the Data Protection Act 1998, this means 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, for the purposes of this Policy, personal data relating to criminal offences and convictions.

staff: the Business’ employees, representatives, agents, consultants, contractors.

Appendix 2: Related policies and procedures

This Policy forms part of a broader Information Governance Framework with other policies listed here. Compliance with these is mandatory.

Any breach of the requirements contained in these documents may result in disciplinary action.

- Information Governance Policy
- Document Management Policy
- Information Security Policy

Further information on data protection policy, procedures and issues, including specific practical guidance on issues of particular relevance to Business staff, can be obtained by contacting dr Roxanne Khan rkhan@onevidence.co.uk