Data Protection Policy

Table of Contents

Data Protection Policy

Table of Contents continued…

Data Protection Policy

Objective and Scope

This Policy sets out the obligations of Prevision Research, a company registered in England under number 6872763, whose registered office is at North House 2, Bond Estate, Milton Keynes MK1 1SW ("the Company") regarding data protection and the rights of survey participants/respondents and business contacts ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

This policy applies to:

- Prevision Research Ltd
- All staff and volunteers of Prevision
- All contractors, suppliers and other people working on behalf of Prevision Research Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998.

This can include:

- Names of individuals
- Postal Addresses
- Email Addresses
- Telephone Numbers
- Payroll data for employees
- …plus any other information relating to individuals

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

Data Protection Policy

Roles, Responsibilities and Authorities

Roles and responsibilities for this policy are shared between the Operations Director, ISMS Representative and the Privacy Officer. These roles share specific responsibility for ensuring threat intelligence is monitored, analysed and actioned in a timely manner.
Where an incident occurs, the senior assigned role taking overall leadership is delegated to the Operations Director.

Legal and Regulatory

Title	Reference
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
Market Research Society Code of Conduct	https://www.mrs.org.uk/pdf/MRS-Code-of-Conduct-2019.pdf
Market Research Society Fair Data Principles	https://www.fairdata.org.uk/10-principles/

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	ISO 27001: 2022 Clause ID	ISO 27002: 2022 Control ID
UK GDPR Compliance Policy				5.34

Related Information

- Change Management Procedure.
- Internal Audit Procedure.
- Document, Data Control and the Protection of Records Procedure.
- Information Security Policy.

Policy

1.1. Governance

1.1.1. Data Protection Officer

- Prevision operate a very small and compact operation.
- Prevision operates as a Data Processor for clients as we have no say over the information to be collected, the manner in which we collect it, the type of respondents we interview, what form the interview takes, what information we collect and how the results are provided.
- Prevision is only a Data Controller in relation to employee data.
- Prevision have an Information Security Officer to handle any data protection issues.

Data Protection Policy

It has been discussed by the Board of Directors and decided that Prevision do not have the resources to appoint a Data Protection Officer at this time.

To demonstrate our commitment to Data Protection we operate an ISO 27001 accredited Information Security Management System which is subject to annual external audits.

1.1.2. Policy Dissemination & Enforcement

The management team Prevision must ensure that all Prevision Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy.

In addition, Prevision will make sure all Third Parties engaged to Process Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by Prevision.

1.1.3. Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

The companies change management policy must be consulted for all new and/or revised systems or processes. The subsequent findings of the risk assessment must then be submitted to the Information Security Officer for review and approval.

1.1.4. Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by Prevision in relation to this policy, an annual Data privacy & GDPR compliance audit will be carried out. Each audit will, as a minimum, assess:

- Compliance with Policy in relation to the protection of Personal Data, including:
    - The assignment of responsibilities.
    - Raising awareness.
    - Training of Employees.
- The effectiveness of Data Protection related operational practices, including:
    - Data Subject rights.
    - Personal Data transfers.
    - Personal Data incident management.
    - Personal Data complaints handling.
- The level of understanding of Data Protection policies and Privacy Notices.

Data Protection Policy

- The currency of Data Protection policies and Privacy Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.
- The adequacy of procedures for redressing poor compliance and Personal Data Breaches.

Any severe issues discovered during the audit process must immediately be reported to the Information Security Officer providing the full audit report. For more detail on our audit procedures see the Internal Audit Procedure.

1.2. Data Protection Principles

Directors and managers of Prevision Research are fully committed to maintaining integrity, confidentiality and availability of the information assets which come under their control.

Data security is taken very seriously which is why Prevision operate an ISO 27001 accredited Information Security Management System that is subject to annual external audits.

Data Protection Policy

1.2.1. Principles of the GDPR

Prevision has adopted the following GDPR principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data. Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data Protection Policy

1.2.2. Principles of the Data Protection Act 1998

Prevision has adopted the following Data Protection principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data Protection Policy

1.2.3. Principles of the MRS Code of Conduct

Prevision is an MRS Company Partner and has adopted the following principles:

1. Researchers shall ensure that participation in their activities is based on voluntary informed consent.
2. Researchers shall be straightforward and honest in all their professional and business relationships.
3. Researchers shall be transparent as to the subject and purpose of data collection.
4. Researchers shall respect the confidentiality of information collected in their professional activities.
5. Researchers shall respect the rights and well-being of all individuals.
6. Researchers shall ensure that participants are not harmed or adversely affected by their professional activities.
7. Researchers shall balance the needs of individuals, clients, and their professional activities.
8. Researchers shall exercise independent professional judgement in the design, conduct and reporting of their professional activities.
9. Researchers shall ensure that their professional activities are conducted by persons with appropriate training, qualifications and experience.
10. Researchers shall protect the reputation and integrity of the profession.

Data Protection Policy

1.2.4. Principles of Fair Data

Prevision is a Fair Data Company and has adopted the following principles:

1. We will ensure that all personal data is collected with customers' consent.
2. We will not use personal data for any purpose other than that for which consent was given, respecting customers' wishes about the use of their data.
3. We will make sure that customers have access to their personal data that we hold, and that we tell them how we use it.
4. We will protect personal data and keep it secure and confidential.
5. We will ensure staff understand that personal data is just that – personal – and ensure that it is treated with respect.
6. We will ensure that the vulnerable and under-age are properly protected by the processes we use for data collection.
7. We will manage our data supply chain to the same ethical standards we expect from other suppliers.
8. We will ensure that ethical best practice in personal data is integral to our procurement process.
9. We will ensure that all staff who have access to personal data are properly trained in its use.
10. We will not use personal data if there is uncertainty as to whether the Fair Data Principles have been applied.

Data Protection Policy

1.3. Data Collection

1.3.1. Data Sources

Prevision holds very little personal information about the people we contact, just enough for the purpose of the survey and no more. Generally, this means we will have a name and a contact phone number or email address and sometimes we will hold information of the geographic location of participants and occasionally some behavioural information. Prevision get respondents contact information from the following sources…

- Customer Lists direct from the client
- Purchased from a list provider
- Publicly available lists e.g. Yell.com
- Pseudonymised survey data
- Employee personal data from the data subject.
- Client contact information.

1.3.2. Data Subject Consent

Prevision will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Prevision is committed to seeking such Consent.

When carrying out our research activities we ensure that we have a legal basis for processing, this is initially ensured in the following ways…

Direct from the client: All clients are required to confirm they have legal grounds for us to contact the data subjects, when commissioning the work, they confirm that they have notified their customers of their legitimate interests to carry out research via their company's privacy policy.

Purchased from a list provider: List providers must provide confirmation that the data subjects they provide contact details for have given consent fairly to be called for market research purposes.

Publicly available lists e.g. Yell.com: Lists of this kind do not identify natural persons and therefore consent is not required.

Pseudonymised survey data: We only go on to interview respondents who give informed consent. When obtaining informed consent, it is important to:

Data Protection Policy

- Determine what disclosures should be made in order to obtain valid consent.
- Ensure the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensure the consent is freely given (i.e. is not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract).
- Document the date, method and content of the disclosures made, as well as the validity, scope, and volition of the consents given.
- Providing a simple method for a Data Subject to withdraw their consent at any time.

Employee personal data: Personal data is collected only from the data subject. It is shared with an external payroll provider which is required to fulfil the employment contract. It is shared with a pension provider which is a legal obligation. To include employee photographs on the company website, informed consent must be obtained. All employee data is securely purged from our systems in line with Previsions data retention policy.

Client contact information: Personal data is collected directly from the data subject. This data is not shared with any third parties and is processed to fulfil the contract. Marketing material is only sent to those that have given informed consent.

1.3.3. External Privacy Notices

Each external website provided by Prevision will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

1.4. Data Use

Identifiable data – Data lists from clients, list providers or public sources are used to contact respondents, it is stored securely, and access is given to only those that need access to complete their job. Identifiable information is only shared with the client if additional informed consent has been obtained direct from the data subject. This data is not shared with any third parties and is securely purged from Prevision systems in line with Previsions data retention policy.

Pseudonymised data - Surveys are conducted with respondents who give informed consent and only a unique identifier is recorded against the interview. When the identifiable data is purged from our systems the survey data becomes anonymous.

Anonymous data - Survey data is shared with the client without any identifiable information attached. Identifiable information is only shared with the client if additional informed consent has been obtained direct from the data subject. This data is not shared with any third parties.

Data Protection Policy

1.4.1. Data Processing

Prevision uses the Personal Data for the following purposes:

- To conduct Market Research
- To fulfil payroll obligations to employees
- To keep clients informed

The use of a data subject's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

For example, it would clearly be within a data subject's expectations that their details will be used by Prevision to respond to a Contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that Prevision would then provide their details to Third Parties for marketing purposes.

Prevision will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Prevision will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for Processing, guidance and approval must be obtained from the Information Security Officer before any such Processing may commence.

Data Protection Policy

In any circumstance where Consent has not been gained for the specific Processing in question, Prevision will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.
- The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller.
- The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.
- The possible consequences of the intended further Processing for the Data Subject.
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation.

1.4.2. Special Categories of Data

Prevision will only Process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

- The Processing relates to Personal Data which has already been made public by the Data Subject.
- The Processing is necessary for the establishment, exercise or defence of legal claims.
- The Processing is specifically authorised or required by law.
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health.

In any situation where Special Categories of Data are to be Processed, prior approval must be obtained from the Information Security Officer and the basis for the Processing clearly recorded with the Personal Data in question.

Where Special Categories of Data are being Processed, Prevision will adopt additional protection measures.

Data Protection Policy

1.4.3. Children's Data

Children are unable to Consent to the processing of their personal data because they may be less aware of the risks involved. Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where Processing is lawful under other grounds, Consent need not be obtained from the child or the holder of parental responsibility.

Should Prevision foresee a business need for obtaining parental consent for services offered directly to a child, guidance and approval must be obtained from the Information Security Officer before any Processing of a child's Personal Data may commence.

1.4.4. Data Quality

Prevision will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by Prevision to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Restriction, rather than deletion of Personal Data, insofar as:
    - a law prohibits erasure.
    - erasure would impair legitimate interests of the Data Subject.
    - the Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

Data Protection Policy

1.4.5. Profiling & Automated Decision-Making

Prevision will only engage in Profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the Data Subject or where it is authorised by law.

Where Prevision utilises Profiling and automated decision-making, this will be disclosed to the relevant Data Subjects. In such cases the Data Subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.
- Object to the automated decision-making being carried out.

Prevision must also ensure that all Profiling and automated decision-making relating to a Data Subject is based on accurate data.

1.4.6. Data Access & Sharing

On receipt of sample data, Prevision will store the data in a password protected encrypted zip file within an encrypted volume on an internal server, which is accessible only by authorised personnel and requires both a virtual password, and a physical USB key to allow access.

The information that is required for the interviewing to take place will then be extracted and allocated to the interviewing stations, this is stored in Voxco and only accessible with the appropriate credentials.
Sample data are checked to ensure that only the information necessary for interviewing to be done is visible to the interviewer.

At all times Active Directory controls who has access to the data store and No Personal data is stored outside of the EU.

1.4.7. Digital Marketing

Prevision will only send promotional or direct marketing material to clients or potential clients that have given informed consent to receive such information via email.

Data Protection Policy

1.5. Data Retention

To ensure fair Processing, Personal Data will not be retained by Prevision for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

The length of time for which Prevision need to retain Personal Data is set out in the Document, 'Data Control and the Protection of Records Procedure'. This takes into account the legal and contractual requirements, that influence the retention periods set forth in the policy. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

1.6. Data Purging

The minimum set of security measures to be adopted when deleting/destroying Personal Data is provided in the Prevision Document, 'Data Control and the Protection of Records Procedure'.

1.7. Data Protection

Prevision will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are Processed.
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where Processing is carried out by a Data Processor, the data can be Processed only in accordance with the instructions of the Data Controller.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that Personal Data collected for different purposes can and is Processed separately.
- Ensure that Personal Data is not kept longer than necessary.

Data Protection Policy

1.8. Data Subject Requests

The Information Security Officer will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, MetaPrivacy will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing to the Information Security Officer and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The use of any automated decision-making, including Profiling.
- The right of the Data subject to:
    - object to Processing of their Personal Data.
    - lodge a complaint with the Data Protection Authority.
    - request rectification or erasure of their Personal Data.
    - request restriction of Processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to the Information Security Officer, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require Prevision to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

Data Protection Policy

If Prevision cannot respond fully to the request within 30 days, the Information Security Officer shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
- The name and contact information of the Prevision individual who the Data Subject should contact for follow up.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Data Protection Policy

1.9. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If Prevision Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If Prevision receives a request from a court or any regulatory or law enforcement authority for information relating to a Prevision Contact, you must immediately notify the Information Security Officer who will provide comprehensive guidance and assistance.

1.10. Data Protection Training

All Prevision Employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, Prevision will provide regular Data Protection training and procedural guidance for their staff.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- The Data Protection Principles set forth in Section 3.2 above.
- Each Employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes.
- The need for, and proper use of, the forms and procedures adopted to implement this policy.
- The correct use of passwords, security tokens and other access mechanisms.
- The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person.
- Securely storing manual files, print outs and electronic storage media.
- The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises.
- Proper disposal of Personal Data by using secure shredding facilities.
- Any special risks associated with particular departmental activities or duties.

Data Protection Policy

1.11. Data Transfers

Prevision may transfer Personal Data to Third Party recipients based within the EU.

Prevision may transfer Personal Data to Third Party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism

Prevision may only transfer Personal Data where one of the transfer scenarios list below applies:

- The Data Subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject. The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.

The minimum set of security measures to be adopted when transferring Personal Data is provided in the Prevision 'Communications (Information Transfer) Security Management Policy '.

Data Protection Policy

1.11.1. Transfers to Third Parties

Prevision will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, Prevision will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, Prevision will enter into, in cooperation with the Information Security Officer, an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

Where the Third Party is deemed to be a Data Processor, Prevision will enter into, in cooperation with the Information Security Officer, an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with Prevision instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches. Prevision has a 'Standard Data Processing Agreement' document that should be used as a baseline template.

When Prevision is outsourcing services to a Third Party (including Cloud Computing services), they will identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include, in cooperation with the Information Security Officer, adequate provisions in the outsourcing agreement for such Processing and Third Country transfers.

1.12. Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Information Security Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Information Security Officer will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Information Security Officer, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

Data Protection Policy

1.13. Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Information Security Officer providing a description of what occurred. Notification of the incident can be made via e-mail iso@previsionresearch.co.uk, by calling 01908 278304, or by using the anonymous incident reporting form at https://prenet.previsioncc.co.uk/compliance.php or https://prenet.previsioncc.co.uk/sampleDatabase

The Information Security Officer will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Information Security Officer will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved. For severe Personal Data Breaches, Prevision will initiate and chair an emergency response team to coordinate and manage the Personal Data Breach response.

Change history and review frequencies

Review frequency of policies and procedural documentation shall be no less than annual and no greater than biennial as determined by the document owner, or immediately after a process /policy change or a policy breach is known to have occurred. Changes shall be documented in the History Table.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N

Data Protection Policy

Appendix A - Information Notification to Data Subjects

The table below outlines the various information elements that must be provided by the Data Controller to the Data Subject depending upon whether or not Consent has not been obtained from the Data Subject.

Information Requiring Notification	With Consent	Without Consent
• The identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative.	✓	✓
• The original source of the Personal Data, and if applicable, whether it came from a publicly accessible source.		✓
• The contact details of the Data Protection Officer, where applicable.	✓	✓
• The purpose(s) and legal basis for Processing the Personal Data.	✓	✓
• The categories of Personal Data concerned.	✓	✓
• The recipients or categories of recipients of the Personal Data.	✓	✓
• Where the Data Controller intends to further Process the Personal Data for a purpose other than that for which the Personal Data was originally collected, the Data Controller shall provide the Data Subject, prior to that further Processing, with information on that other purpose.	✓	✓
• Where the Data Controller intends to transfer Personal Data to a recipient in a Third Country, notification of that intention and details regarding adequacy decisions taken in relation to the Third Country must be provided.	✓	✓
• The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.	✓	✓
• Where applicable, the legitimate interests pursued by the Data Controller or by a Third Party.	✓	✓
• The existence of Data Subject rights allowing them to request from the Data Controller- information access, objection to Processing, objection to automated decision-making and profiling, restriction of Processing, data portability, data rectification and data erasure.	✓	✓
• Where Processing is based on Consent, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal.	✓	
• The right to lodge a complaint with a Data Protection Authority.	✓	✓
• The existence of automated decision-making (including Profiling) along with meaningful information about the logic involved and the significance of any envisaged consequences of such Processing for the Data Subject.	✓	✓
• Whether the provision of Personal Data is a statutory or contractual requirement, a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and if so the possible consequences of failure to provide such data.	✓	✓

Appendix B - Adequacy for Personal Data Transfers

Data Protection Policy

The following are a list of countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data.

- EU Countries
  (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK)
- Iceland
- Liechtenstein
- Norway
- Andorra
- Argentina
- Canada (commercial organisations)
- Faeroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
- United States (Privacy Shield certified organisations)

The following are a list of Third Country transfer mechanisms that can provide adequate protection when transfers are made to countries lacking an adequate level of legal protection.

Appropriate safeguards

- Model Clauses
- Binding Corporate Rules
- Codes of Conduct
- Certification Mechanisms

Derogations

- Explicit Consent
- Compelling Legitimate Interests
- Important reasons of Public Interest
- Transfers in response to a foreign legal requirement
- DPA approved contracts between Data Controllers and Data Processors