Protection of Personally Identifiable Information Records Policy

Objective and Scope

The objective of the Prevision Research Protection of PII Records Policy is to demonstrate the company's commitment to respecting and protecting privacy and personal information records by fully complying with the General Data Protection Regulation (GDPR) in relation to PII records retention and destruction.

This policy should be read in conjunction with the Privacy Policy for matters related to collection, use and protection of PII.

Protection of PII Records

Records management of personally identifiable information is about the records of an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.

Roles, Responsibilities and Authorities

Roles and responsibilities for this policy are assigned to the Operations Director. This role shall take responsibility for ensuring policy is in compliance with the General Data Protection Regulation (GDPR) including record retention and destruction.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

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

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**
PII Records Protection				5.34

Related Information

- Information Security Policy
- Privacy Policy

Protection of Personally Identifiable Information Records Policy

- Data Protection Policy

Policy

Prevision Research only stores or retains personal information for purposes directly related to Prevision Research business, or otherwise as a result of a specific engagement. Destruction of PII records is undertaken according to the rules related to its initial collection and the laws of the jurisdiction in which it was collected.

This policy covers Prevision Research storage, retention and destruction of personally identifiable information that we gather during the course of Prevision Research business activities, including that from our website.

This policy does not apply to the practices of companies that Prevision Research does not own or control.

How personally identifiable information is stored

Prevision Research are committed to ensuring the security of stored PII information to prevent unauthorised access or disclosure, maintain data accuracy, ensure the appropriate use of procedures to safeguard and secure the information and/or destroy under a secure environment.

The following standards shall be met:

1. Records shall be named in a manner that provides identification sensitivity and retention period without compromising personal identifiable information.
2. Secure storage protection according to the information classification policy and regulatory obligations for PII such as GDPR etc.
3. Electronic storage of PII data shall enable retrievability within specified timelines only from the authorised PII owner or delegate.
4. Encrypted PII records shall have cryptographic keys and programs associated with encrypted archives, shall be retained to enable decryption of the records only under agreed PII authority for the length of time the records are retained.

Use of appropriate encryption when transferring or holding sensitive data

Any personal information Prevision Research stores is held on our internal network. These systems are password protected, encrypted and, where required, only limited authorised persons are permitted to access or destroy the information.

Prevision Research are also required to comply with UK government policies in relation to storage and secure destruction of information.

Prevision Research may use third parties to store some PII on servers in the UK or overseas, but only where steps have been taken to ensure that the third parties comply with Prevision Research's privacy obligations and where to do so does not breach Prevision Research's obligations to our clients and website users. Third parties are required to store data in an encrypted format.

Protection of Personally Identifiable Information Records Policy

Your rights in relation to PII being held by Prevision Research

You have certain rights regarding the storage and destruction of your PII. To submit a request in respect of your rights, please email mailto:iso@previsionresearch.co.uk

Please note that Prevision Research may not be able to fully comply with your request, if it is frivolous or impractical, if it jeopardises the rights of others, or if it is not required by law. In those circumstances, Prevision Research will still respond to notify you of such a decision.

You may also need to provide Prevision Research with additional information, which may include further personal information, if necessary, to verify your identity and the nature of your request.

Your rights in regards to records and erasure include:

- Access. You can request access to the personal information Prevision Research held about you and request a copy of the same.
- Rectification. If you believe that any personal information Prevision Research is holding about you is incorrect or incomplete, you can request that Prevision Research correct or supplement such data.
- Erasure. You can request that Prevision Research erase some or all of your personal information from their systems.

Destruction of PII records held by Prevision Research

On the request of the owner of PII content, when the information is no longer able to be stored legally or no longer required, the PII information is deactivated and then anonymised.

Do not attempt to use a delete key function and then remove from the 'trash bin' as this is not safely removed and can be re-established and retrieved.

The effective way other than the computer automatically writing over the disk space when you download a new application is to:

- Macintosh: Use the built-in utility program to completely remove deleted files from the hard drive. This must be installed and used for all PII data then select 'Secure Empty trash'.
- Windows: Install a third party software wiping program that can cleanse unallocated disk space.

Emails

Secure email deletion processes are only effective if both the receiver and sender remove the email permanently. Removing an email permanently requires the mechanism for email recovery to be permanently disabled. For this reason, PII related data should never be sent or allow it to be received via email unless encrypted.

Backups of PII information

When deleting files off a network, archived data will also require deletion if full deletion is to be achieved. This includes time machine, cloud, external hard drives, CD/DVDs, email, server and offsite backups.

Protection of Personally Identifiable Information Records Policy

If you have a complaint, request or query

If you wish to communicate with a representative about the storage of your data please contact:

- iso@previsionresearch.co.uk, or
- 01908 278 303

This policy is current as at 01/05/2024 and is subject to change as Prevision Research update our privacy obligations. Prevision Research recommend that you check this page regularly to monitor any changes to this policy.

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change or a policy breach is known to have occurred.

Periodic reviews shall take into account feedback from management reviews, regulatory changes and audits. Changes to the policy must be approved by a senior executive then communicated to all previous persons or organisations with access to the policy. Refer below for the most recent review.

Refer below for the most recent review.

History table

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