GDPR and Privacy Policy

helpmypension t/a helpmypension.ie

Helpmypension needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards thus complying with the legislation.

Purpose

This data protection policy ensures Helpmypension:

- Comply with Data Protection Legislation and follow Good Practice;
- Protect the Rights of Employees, Customers and Partners;
- Is Transparent in terms of How It Stores and Processes Individuals' Data;
- Protects itself from the Risks associated with a Data Breach.

Scope

Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Policy Statement

The General Data Protection Regulation (GDPR) describes how organisations — including helpmypension, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR Is Underpinned by Six Important Principles Requiring That Personal Data Be:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified, explicit and legitimate purpose;
3. Adequate, relevant and limited to what is necessary;
4. Accurate and where necessary, kept up to date;
5. Retained only for as long as necessary;
6. Processed in an appropriate manner to maintain security.

The Board of Directors of helpmypension, located at 208 Meadowview, Drogheda are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of

individuals whose information Helpmypension collects and processes in accordance with the General Data Protection Regulation (GDPR).

The GDPR and this policy are applicable to all helpmypension personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

The GDPR Owner is responsible for reviewing the register of data processing annually, in light of any changes to helpmypension activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments (DPIA's).

Partners and any third parties working with or for helpmypension, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.

No third party may access personal data held by helpmypension without having first entered into a data confidentiality agreement which imposes obligations on the third party no less onerous than those to which helpmypension is committed, and which gives helpmypension the right to audit compliance with the agreement.

Privacy Policy — Data Protection Principles

1. Be Processed Lawfully, Fairly and in a Transparent Manner

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the Data Protection Officer;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

2. Personal Data Can Only Be Collected for Specific, Explicit and Legitimate Purposes

- Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of helpmypension's GDPR register of processing.

3. Personal Data Must Be Adequate, Relevant and Limited to What is Necessary

- The Data Protection Officer*/GDPR Owner is responsible for ensuring that helpmypension do not collect information that is not strictly necessary for the purpose for which it is obtained.
- All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to a privacy statement and be approved by the Data Protection Officer*/GDPR Owner.
- The Data Protection Officer*/GDPR Owner will ensure that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

4. Personal Data Must Be Accurate and Kept Up to Date

- Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
- The Data Protection Officer* is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
- It is also the responsibility of the data subject to ensure that data held by helpmypension is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.
- The Data Protection Officer*/GDPR Owner is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

** Recent advice received indicates that small brokers, those which are local rather than nationwide or do not have a large network of offices/brokers covering more than one county, are not likely to be required to appoint a DPO. A possible rule of thumb is customer numbers, so those in the hundreds rather than thousands are likely to be considered small for the purpose of this requirement.*

- On at least an annual basis, the Data Protection Officer*/GDPR Owner will review the retention dates of all the personal data processed by helpmypension, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose.

5. Personal Data Must Be Kept Only for as Long as Necessary

- Where personal data is retained beyond the processing date, it will be minimised, encrypted/pseudonymised, in order to protect the identity of the data subject, in the event of a data breach.
- Personal data will be retained in line with the Retention of Records Procedure and, once its retention date has passed, it must be securely destroyed, as set out in this procedure.
- The Data Protection Officer*/GDPR Owner must specifically approve any data retention that exceeds the retention periods defined in the Retention of Records Procedure, and must ensure that the justification is clearly identified, and in line with the requirements of the data protection legislation. This approval must be in written format.

6. Processed in an Appropriate Manner to Maintain Security

In determining appropriateness, the Data Protection Officer*/GDPR Owner should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on helpmypension itself, and any likely reputational damage, including the possible loss of customer trust.

When assessing appropriate **technical measures**, the Data Protection Officer*/GDPR Owner will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;

- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisation's premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to helpmypension.

When assessing appropriate **organisational measures**, the Data Protection Officer*/GDPR Owner will consider the following:

- The appropriate training levels throughout helpmypension;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employees' own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations, to take appropriate security measures when transferring data outside the EEA.

These controls have been selected, based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.