Data Protection Policy

Contents

INTRODUCTION **2**

PURPOSE & SCOPE **2**

ROLES, RESPONSIBILITIES & STAFF DUTIES: **4**

DEFINITIONS: **5**

STATEMENT **6**

1. STRUCTURE OF THE POLICY **10**

1.1 PROCESSING OF PERSONAL DATA 11
1.2 INTERNAL USER GUIDE 11

2. CONSENT **11**

2.1 POLICY 12
2.2 PROCEDURE 12
2.3 WITHDRAWAL 12

3. ACCESS TO DATA **13**

3.1 DATA SUBJECT ACCESS 13
3.2 (A) TRANSFERS – UK 14
(B) TRANSFERS - CANADA 14
3.2 REQUEST PROCEDURE 14

4. PRIVACY **16**

4.1 POLICY & PROCEDURE 16
4.2 PRIVACY NOTICE 16

5. PERSONAL DATA BREACH NOTIFICATION **17**

5.1 POLICY 17
5.2 PROCEDURE 17

6. DATA PROTECTION IMPACT ASSESSMENT (DPIA) **18**

6.1 POLICY 18
6.2 PROCEDURE 19
6.2.1 Data Processing (Data Flow) *19*
6.2.2 Privacy Risks *20*
6.2.3 Prior Consultation (Article 36, GDPR) *20*

7. RETENTION OF RECORDS **20**

THE MANAGERS ARE RESPONSIBLE FOR ENSURING THAT RETAINED RECORDS ARE INCLUDED IN BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS. 21
7.1 POLICY 21
7.2 PROCEDURE 21

8. SUB CONTRACT PROCESSING **22**

8.1 POLICY 22

8.2 PROCEDURE 22
REVIEW 22
APPENDICES 23
APPENDIX – GUIDANCE 23

Revision History:

No	Author/Reviewer	Date	Status (Draft/Published)	Comment
1.0	Historic log	18-Jan-12	Draft/Publish	Old Data protection Policy
2.0	Historic log	1-Jan-18	Amendment	New GDPR Policy draft based upon articles.
3.0	Historic log	Apr-18	Review/amend	Overall review in-line with GDPR/customers/HR and other subjects.
4.0	Historic log	May-18	Approved	

5.0	Historic log	May-19	Annual Review	Update references from DPA1998 to DPA2018
6.0	Historic log	Jun-20	Published	Annual Review
7.0	Historic log	Feb - 22	Published	Annual Review
7.1	Anika Browne	May-22	Published	Layout update
8&9	Ricardo Pombo	Jan – 23	Published	Document Review
10.0	Ricardo Pombo	Feb-24	Published	Update on retention of information
11.0	Anika Browne / Ricardo	Mar-25	Published	Policy review – Incorporate US & Canada laws
11.1	Ricardo Pombo	Mar-26	Published	Annual review – no changes

Introduction

This policy outlines our commitment to protecting personal data in compliance with applicable data protection laws in the UK, USA and Canada, specifically in Toronto and Quebec.

In order to operate efficiently, Peoplesafe and its subsidiary companies (incorporating OK Alone) collect information about people with whom we work. These may include members of the public, current, past and prospective employees, customers and suppliers.

Peoplesafe ensures compliance with the following legislation:

GDPR (UK)

PIPEDA (Canada)

Act Respecting the Protection of Personal Information in the Private Sector (Law 25)- (Quebec)

FTC Act - Federal Trade Commission, USA

HIPPA (USA)

Colado Privacy Act (Colorado)

This personal information must be handled properly in accordance with current data protection legislation. Legislation regulates the way that we handle 'personal data' that we collect to carry out our functions and gives certain rights to employees, contractors, customers and people whose 'personal data' we may hold.

We consider that the correct treatment of personal data is integral to our successful operations and to maintaining trust of the persons we deal with. We fully appreciate the underlying articles and principles of legislation(s) and support and adhere to its provisions

Purpose & Scope

Appropriate legislation have been taken into account in the preparation of this policy for the purposes of regulating the use by those who obtain, hold and process personal data on living individuals, of those personal data.

Please see below table regarding compliance requirements based on country requirements:

Legislation	Applicable Country	Legislation requirements
GDPR	United Kingdom	• Only hold personal information for the purpose for which it is registered with the ICO • Delete that information when no longer required • Have appropriate security to protect that information against unlawful or unauthorised use or disclosure, accidental loss, destruction or damage • Process personal data lawfully fairly and transparently. • Respect an individuals have rights to access, rectify and delete personal date
DPA 2018	United Kingdom	• Follow lawful data processing principles • Ensure strong security measures • Handle sensitive date with extra care
Federal Trade Commission	United States	• Data collected should be handled fairly, transparently and securely. • We must correctly represent how we collect, use or protect consumer data. • Implement reasonable security practices to prevent data breaches.
HIPAA	United States	• If handing protected health information we must comply with HIPAA regulations. • Ensure the confidentiality, integrity and security of health data. • Safeguards for the prevention of unauthorized access. • Provide individuals with rights to access and correct information
Colardo Privacy Act	United States (Colorado)	• Provide clear and accessible privacy notices explain how personal data is collected, used and shared. • Allow consumers the right to access, correct and delete their personal data. • Allow the consumer to opt out of targeted advertising ad data sales. • Completion of risk assessment for high-risk processing activities • Protect consumer date through the implementation of security controls.
PIPEDA	Canada	• Explicit consent must be provided prior to collecting a processing personal data • Safeguard personal information whilst allowing individuals to access, correct data. • Implement accountability measures in order to remain in compliance with this law
Quebec Law 25	Canada (Quebec)	• Obtain explicit consent prior to collecting or processing personal data. • Provide individuals with the right to access, correct, and transfer data. • Appoint a privacy officer to conduct privacy impact assessments and implement strong security measures.

		• Notify authorities and affected individuals promptly in the case of a data breach posing a risk of harm

In particular, GDPR sets the scope of policy to:

Material scope (GDPR Article 2)

The GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (GDPR Article 3)

The GDPR will apply to all controllers that are established in the EU who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data to offer goods and services or monitor the behaviour of data subjects who are resident in the EU.

Applicability to Employees and Outsourced Suppliers

The GDPR and this policy apply to all employees of Peoplesafe, including outsourced suppliers. For the purposes of this policy, the term "Staff" includes all members of Peoplesafe, such as permanent, fixed-term, and temporary staff, secondees, third-party representatives, agency workers, volunteers, interns, agents, and sponsors engaged with Peoplesafe in the UK or overseas

This policy also applies to all members of staff employed by any of Peoplesafe's subsidiary companies. This policy also applies to all Peoplesafe's 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.

Any breach of the above legislations or this policy will be dealt with under Peoplesafe's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for Peoplesafe, 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 Peoplesafe without having first entered into a data sharing agreement, which imposes on the third-party obligations no less onerous than those to which Peoplesafe is committed, and which gives Peoplesafe the right to audit compliance with the agreement.

This policy applies to all personal and sensitive personal data processed on computers and stored in manual (paper based) files. It aims to protect and promote the rights of individuals and Peoplesafe.

Roles, Responsibilities & Staff Duties*:*

All staff members are responsible for adhering to this policy and ensuring that personal data is handled in compliance with the above legislations.

Under the GDPR, Peoplesafe acts as a Data Processor. All staff are made aware of their duties and responsibilities during their induction training. Top management and all those in managerial or supervisory

roles throughout Peoplesafe are responsible for developing and encouraging good information handling practices within Peoplesafe; responsibilities are set out in individual job descriptions. Top Management should assign the responsibilities of Data Protection / Privacy Officer (DPO)

/PO) to an authorised member of the staff who is competent with the data handling, systems, and general process implementation.

The DPO/PO is responsible for reviewing the register of processing annually in the light of any changes to Peoplesafe's activities and to any additional requirements identified by means of data protection impact assessments. DPO's accountability includes:

- Development and implementation of the GDPR as required by this policy; and
- Security and risk management in relation to compliance with the policy.

DPO/PO, who the Directors consider to be suitably qualified and experienced, has been appointed to take responsibility for the company's compliance with this policy on a day-to-day basis and has direct responsibility for ensuring that Peoplesafe complies with the GDPR, as do Manager/Executive (generic/line)'s in respect of data processing that takes place within their area of responsibility.

The DPO/PO has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

Compliance with data protection legislation is the responsibility of all employees/staff of Peoplesafe who process personal data. Company's training Policy sets out specific training and awareness requirements in relation to specific roles and employees/staff of Peoplesafe generally.

Employees/Staff are responsible for ensuring that any personal data about them and supplied by them to Peoplesafe is accurate and up to date. Peoplesafe is registered under the register kept by the Information Commissioner Office.

Definitions:

For information held by Peoplesafe, personal data essentially means any recorded information held by us and from which a living individual can be identified. It will include a variety of information including names, addresses, telephone numbers, photographs of people and other personal details. It will include any expression of opinion about a living individual or any indication of our intentions about that individual. The categorised definition from GPDR (Article 4) are described below.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, 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 person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual or the customer under agreement who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Agreement – the principal agreement/contract between the data subject and data processor.

Statement

The Board of Directors and Senior management of Peoplesafe are committed to safeguarding the privacy of personal data and ensuring compliance with GDPR and the applicable country legislations as outlined above.

Peoplesafe is committed to compliance with all relevant EU and Member State laws in respect of personal data, and data protection rights of individuals whose information Peoplesafe collects and processes in accordance with the General Data Protection Regulation (GDPR), DPA 2018, PIPEDA,HIPAA and Quebec. S Law 25.

Compliance with the GDPR is described by this policy and other relevant systems & governing policies such as the Security manual, IG Policy and the IS Policy, along with connected processes and procedures.

As per Article 5 & 6 of the GDPR requirements and data protection's basic principles; Peoplesafe complies with the following enforceable data protection principles by making sure that personal data is:

1. **Fairly and lawfully processed (GDPR Article 6: Lawfulness of processing)**

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent and agreements.

Fairly – for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 & 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 governance of company's Privacy Notice Procedure is set out in a section below of this Policy (Privacy).

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 DPO/PO;
- 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. **Processed for limited purposes**

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. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority.

3. **Adequate, relevant, and not excessive**

Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the DPO.

4. **Accurate and where necessary 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.
- It is also the responsibility of the data subject to ensure that data held be 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.
- All audience as defined in the scope should be required to notify Peoplesafe of any changes in circumstance to enable personal records to be updated accordingly.
- The DPO/PO 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.
- On at least an annual basis, the DPO/PO will review the retention dates of all the personal data processed by Peoplesafe by reference to the data inventory and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted in line with IS Policy
- The DPO/PO is responsible for responding or assisting HR, to the requests for rectification from data subjects. This can be extended to a further two months for complex requests. If Peoplesafe decides not to comply with the request, the DPO/PO must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.
- The DPO/PO is responsible for making appropriate arrangements that, where third-party companies may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where required.

5. **Not kept longer than necessary**

- Where personal data is retained beyond the processing date, it will be protected appropriately.
- Personal data will be retained in line with Peoplesafe retention policies.
- Personal data will be retained on the basis of lawful grounds for processing data, that may be relevant to its processing of HR data, including the processing activity will be "*necessary for the performance of a contract"* or because the processing is necessary for *"compliance with a legal obligation" or* for the purposes of *"legitimate interests"* pursued by the business

- The DPO/PO must specifically approve any data retention that exceeds the retention periods and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

6. Processed in accordance with the individual's rights

Data subjects, under the agreement of retention, have the number of rights regarding your data and it's processing including the right to be informed, erasure, rectification, right to restrict processing and automated profiling

Peoplesafe ensures that data subjects may exercise these rights to complain to Peoplesafe related to the processing of their personal data, the handling of a request from a data subject.

7. Consent

- Peoplesafe understands 'consent' to mean that it has been under the agreement, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent in certain circumstances which will not affect the lawfulness of the processing before your consent was withdrawn.
- Peoplesafe understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement.
- Privacy notice acts as a form of active communication between the parties to demonstrate active consent which cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.
- For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.
- In most instances, consent to process personal and sensitive data is obtained routinely by Peoplesafe using agreed documents.

8. Secure

I.e. appropriate organisational and technical measures shall be taken against unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.

9. Disclosure of Data

- Peoplesafe must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police.
- All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO/PO and/or HR.

10. Not transferred to countries outside the European Economic area unless the country to which the data is to be transferred has adequate level of protection for the individuals.

11. Data Inventory

Peoplesafe has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project; this inventory should include:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

1. Structure of the Policy

Peoplesafe gains and holds the data necessary for the maintenance of its business. In broad terms, "the data" means information which is being processed by means of equipment operating automatically in response to instructions given for that purpose; or, which is recorded with the intention that it should be processed by means of such equipment; or, is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

Data can be any personal information which relates to a living individual who can be identified. This includes any expression of opinion about the individual. Such data falls into two main groups of purposes to which Peoplesafe's data protection policy is structured.

1. External purposes. Data held on behalf of customers to enable Peoplesafe to provide the services.
2. Internal purposes.
    a. Data about customers used for sales, marketing, support, statistical and financial purposes.
    b. Data about employees for management purposes.

The service is provided on an agreed understanding that the customer, as the owner of the personal data relating to those for whom the service is provided, has decided that Peoplesafe should hold the personal data in its alarm management database. The customer, as Data Controller, has further decided that Peoplesafe should process that data on behalf of the customer for the purpose of managing incidents derived from personal safety alarms. Peoplesafe therefore acts as the Data Processor.

In the event of a customer terminating the service, Peoplesafe undertakes, with one exception, to remove the data from its database when no longer required. The exception is for personal and alarm information relating to real incidents where there may be a requirement for evidence at a later stage. Peoplesafe accepts that in this situation Peoplesafe becomes the Data Controller. This information will be deleted after three years following contract termination.

The customer should be satisfied that the personal data they provide is used for the correct purpose and it is Peoplesafe's responsibility to ensure the data is secure and used only for the purpose for which it is provided.

Peoplesafe's Terms & Conditions refer to these responsibilities, for both Peoplesafe and the customer. The sales process is to make clear to customers their responsibilities in this regard.

Should customers wish to extend the period for which personal data is retained that written agreement must be held.

Peoplesafe retain the staffs' data on an agreed understanding that the data will be processed under the agreement to comply with the employment, any legal requirements, pursue the legitimate interests of Peoplesafe and protect our legal position.

1.1 Processing of personal data

In this context, 'processing' is used in narrow sense of editing, amending, or querying the data which is stored with Peoplesafe systems. Peoplesafe should process that data on behalf of the customer for the purpose of managing the provided services under the agreement

Personal data must not be processed except for those purposes for which they were obtained or for a similar, analogous purpose such as alarm management.

1.2 Internal User Guide

For the purposes of sales, marketing, customer service, customer statistics, finance, and employee management, Peoplesafe acts as the Data Controller. This means we decide the purpose for which we hold the data, register that purpose with the Information Commissioner, and ensure it is secure, appropriate, and used only for the purposes for which we have decided it is to be held.

The purpose for which we hold this data is given in our Register Entry with the Information Commissioner.

Staff will be required to ensure that where such personal data is held that it is essential for the purpose and is held no longer than is necessary for that purpose.

Once that data is no longer necessary for the purpose for which it was gained it should be deleted from all computer systems and paper files unless there is a compelling reason to retain it.

Some information, particularly financial, is to be retained as required by various statutory requirements.

Peoplesafe will ensure that at least one of the following conditions are met before we process any personal data including but not limited to information about racial or ethnic origin, political opinions, religious and other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings, or convictions:

1. the customer or staff has consented to the processing via company agreement(s).
2. the processing is necessary for the performance of a contract with the individual or a customer
3. the processing is required under a legal obligation (other than one imposed by a contract)
4. the processing is necessary to protect vital interests of the individual
5. the processing is necessary to carry out public functions e.g. administration of justice
6. the processing is necessary in order to pursue our legitimate interests or those of third parties (unless it could unjustifiably prejudice the interests of the individual)

2. Consent

The consent of the data subject is defined by the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Specific conditions apply to the validity of consent given by children in relation to information society services, with requirements to obtain and verify parental consent below certain age limits.

2.1 Policy

Those who wish obtain personal data must comply with the guidelines issued from time to time by Peoplesafe and, in particular, should tell data subjects via privacy notice, agreement or other form of relevant document(s), the purpose for which they are gathering the data, obtain their consent, and inform them that Peoplesafe will be processing the data either as a Data Controller or data processor for the purpose of the GDPR regulation and identities of any other persons to whom the data may be disclosed.

No more data should be collected than is necessary for the purpose(s) declared.

Peoplesafe demonstrates data subject(s) consent is intelligible and accessible using clear and plain language.

Peoplesafe demonstrates processing of data is limited to that stated in the contract, bound by the explicit consent given by the data subject.

2.2 Procedure

Peoplesafe provides a clear Privacy notice wherever personal data is collected (refer to Section 7 – Privacy) where Data Subjects are made aware of what data is collected and the purpose of the use of that data. Data Subjects are also made aware of their rights in relation to their personal data.

Peoplesafe demonstrates Data Subject(s) consent to the processing of any type of his or her personal data through the means of agreement and/or a Staff Data Subject Consent acknowledgement form; and returns it back to the relevant person.

Peoplesafe demonstrates data subject(s) consent is clearly distinguishable from any other matter relating to the data subject (if recorded in paper / electronic file format use Data Subject Consent

Form, or if consent was provided via email then the email is attached to the Data Subject Consent form).

Peoplesafe ensures Data Subject(s) are informed of their right to withdraw consent as per the agreement at any time on the Data Subject Consent form.

2.3 Withdrawal

This procedure addresses the data subject(s) right to withdraw consent for the processing their personal data which will not affect the lawfulness of the processing before your consent was withdrawn. Whereas consent covered all processing activities carried out for the same purpose or purposes, withdrawal of consent covers all processing activities carried out for the same purpose or purposes.

In the event that a Data Subject wished to withdraw their consent; the Data Subject, where company is acting as a data processor, would need to abide by the agreement; and, where company is acting as a controller (i.e. for staff) would need to request in written to HR or the DPO; which would then be reviewed before a confirmation would be provided to the Data Subject that processing of data has now stopped.

As per the agreed contract with the customer; any data held on the Data Subject will be disposed of accordingly. Peoplesafe ensures that a representative acknowledges the Data Subjects request and Peoplesafe chooses whether to request that the data subject provide evidence of their identity

- Peoplesafe does not by default accept and process personal data received from another data controller following a personal data request nor does it retain all the data received.
- Peoplesafe only accepts and retains data that is necessary and relevant to the service being provided.
- If data received contains third-party data, Peoplesafe keeps the data under the sole control of the requested user or the customer. This data is only managed for their needs and not for other purposes of Peoplesafe. This other purpose could be marketing needs.

3. Access to Data

3.1 Data Subject Access

All personal data processed by Peoplesafe is within the scope of this procedure.

Policy & Procedure

Peoplesafe is fully committed to facilitating access by various groups of applicants such as staff, data subjects and customers to personal data, while bearing in mind the need to protect other individuals' rights of privacy.

Under the agreement, the data subjects are entitled to obtain:

- Confirmation as to whether Peoplesafe is processing any personal data about that individual;
- Access to their personal data;
- Any related information;
- In the case of data processor, company obligations are with the customers under the agreement.

Peoplesafe's policy is to exercise its discretion under the legislation to protect the confidentiality of those whose personal data it holds.

- External requests for personal information and about customers regarding the provision of the service are to be referred to the DPO/PO for a decision.
- Apart from the purpose of carrying out our obligations under the Agreement, the employees of Peoplesafe may not disclose any specific information of employees, customers (which may reveal personal data), including information as to whether or not any person is or has been a customer or employee unless they are clear that they have been given authority by Peoplesafe to do so.
- No employee may disclose personal data to the police or any public authority unless the disclosure has been authorised.

Access Control Policy and Personal Data Management of Peoplesafe's IS Policy identifies established Access control, policy and personal data management policy.

Data Subjects' Rights

Data subjects, under the agreement of retention, have the number of rights regarding your data and its processing including the right to be informed, erasure, rectification, right to restrict processing and automated profiling, right to prevent processing for the purpose of direct marketing, and to have personal data provided to

them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
Data subjects have the right to complain to Peoplesafe related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure under the agreement.

Legal requirements
While it is unlikely, Peoplesafe may be required to disclose personal data by a court order or to comply with other legal requirements. We will use all reasonable endeavours to notify you before we do so, unless we are legally restricted from doing so.

No commercial disposal to third parties
Peoplesafe shall not sell, rent, distribute or otherwise make personal data commercially available to any third party,

3.2 (a) Transfers – UK
Under the agreement, the data subject agrees to control its data into company's systems. Peoplesafe undertakes not to change, edit or delete this information unless requested by the customer to do so, or on contract termination. This is to be requested in writing.

Personal data should not be transferred outside Peoplesafe, and not to a country outside the EEA

I. except with the customer's consent; or
II. Adequate safeguards have been put in place in consultation with IS Group, it is established that other derogations apply.

(b) Transfers - Canada
Personal data is stored on servers located in Toronto, Canada, with backup servers in Quebec, Canada. We ensure that any cross-border data transfers comply with GDPR requirements by using Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) to provide adequate safeguards.

(c) Transfers – USA

Personal data is stored on servers located in the United States. We ensure that any cross-border data transfers comply with applicable US data protection laws and regulations, such as the Federal Trade Commission (FTC) Act and the Health Insurance Portability and Accountability Act (HIPAA). To provide adequate safeguards, we use Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) where necessary. Additionally, we implement robust security measures to protect personal data against unauthorized access, disclosure, alteration, and destruction.

3.2 Request Procedure

Subject Access Requests are made using the Subject Access Request form. These requests are logged on Peoplesafe CRM system and handled by the relevant departments as per the department processes.

The data subject specifies to Peoplesafe specific set of data held by Peoplesafe on their subject access request (SAR). Peoplesafe maintains a Subject Access Request Log. The data subject can request all data held on them.

Peoplesafe records the date that the identification checks (if applicable) were conducted, and the specification of the data sought.

Peoplesafe provides the requested information to the data subject within one month from this recorded date.

Once received, the subject access request (SAR) application is immediately forwarded to the DPO/PO, who will ensure that the requested data is collected within the specified time frame. Collection entails:

I. Collecting the data specified by the data subject, or
II. Searching all databases and all relevant filing systems in Peoplesafe, including all back up and archived files and all email folders and archives. The DPO/PO maintains a data map that identifies where all data in Peoplesafe is stored.

The DPO/PO maintains a record of requests for data and of its receipt, including dates.

The DPO/PO reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed.

If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:

- National security
- Crime and taxation
- Health
- Education
- Social Work
- Regulatory activity
- Journalism, literature and art
- Research history, and statistics
- Publicly available information
- Corporate finance
- Examination marks
- Examinations scripts
- Domestic processing
- Confidential references
- Judicial appointments, honours and dignities
- Crown of ministerial appointments
- Management forecasts
- Negotiations

- Legal advice and proceedings
- Self-incrimination
- Human fertilization and embryology
- Adoption records
- Special educational needs
- Parental records and reports

If a data subject requests Peoplesafe to provide them with the personal data stored by the controller/processor, then Peoplesafe will provide the data subject with the requested information in electronic format, unless otherwise specified. Peoplesafe will act in an agreed time period to address the data subject requests and will advise accordingly.

Under the agreement, Peoplesafe may include the cost arrangement to assist the complex requests.

4. Privacy

4.1 Policy & Procedure

All processing of personal data by Peoplesafe is within the scope of this procedure.

The DPO/PO is responsible for ensuring that the privacy notice(s) is correct and that mechanisms exist such as having the Privacy Notice(s) on Peoplesafe's website(s), employment handbook and other documents to make all data subjects aware of the contents of this notice prior Peoplesafe's commencing collection of their data.

All staff/Employees that need to collect personal data or interact with Data Subjects are required to adhere to the requirements of this procedure and are responsible for ensuring that the Privacy Notice is drawn to the Data Subject's attention.

Peoplesafe identifies the legal basis for processing personal data before any processing operations take place by clearly establishing, defining and documenting:

The specific purpose of processing the personal data and the legal basis to process the data under:

- Necessary for employment rights or obligations;
- performance of a contract where the data subject is a party;
- legal obligation that Peoplesafe is required to meet;
- protect the vital interests of the data subject, including the protection of rights and freedoms;
- official authority of Peoplesafe or to carry out the processing that is in the public interest;
- Necessary for the legitimate interests of the data controller or third party, unless the processing is overridden by the vital interests, including rights and freedoms;
- preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, provision of health or social care treatment, or management of health and social care systems and services, under the basis that appropriate contracts with health professionals and safeguards are in place;
- public health, ensuring appropriate safeguards are in place for the protection of rights and freedoms of the data subject, or professional secrecy;
- National laws in terms of processing genetic, biometric or health data.

4.2 Privacy Notice

The General Data Protection Regulation (2016/679 EU) (GDPR) requires Peoplesafe to issue a privacy notice to the following data subjects:

- Customers

- Staff and employees

- Other data subjects such as job applicants.

The customer and job applicant specific privacy notices are in the public domain and should be available on company website(s).

The staff privacy notice is an HR controlled document and should be available to staff in the employment handbook. It is mandatory for the staff that they provide their acknowledgement to HR department.

5. Personal Data Breach Notification

5.1 Policy

This procedure applies in the event of a personal data breach under Article 33 of the GDPR – Notification of a personal data breach to the supervisory authority – and Article 34 – Communication of a personal data breach to the data subject.

The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is data controller, or a data processor for the same data processing activity; or whether it is a joint controller.

Unlawful obtaining or disclosure of personal data (including the transfer of data outside EEA) or any other breach under article 33 of the GDPR by staff will be treated seriously by Peoplesafe and may lead to disciplinary action up to and including suspension or dismissal.

This policy should be read in line with Incident (Breach) Policy as described in Peoplesafe's IS Policy.

5.2 Procedure

5.2.1 Supervisory Authority Notification

Peoplesafe determines if the supervisory authority need to be notified in the event of a breach.

Peoplesafe assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting data protection impact assessment against the breach.

If a risk to data subject(s) is likely, Peoplesafe reports the personal data breach to the supervisory authority Information Commissioners Office without undue delay, and not later than 72 hours.

If the data breach notification to the supervisory authority is not made within 72 hours, Peoplesafe's DPO/PO submits it electronically with a justification for the delay.

If it is not possible to provide all the necessary information at the same time Peoplesafe will provide the information in phases without undue further delay.

The following information needs to be provided to the supervisory authority:

- A description of the nature of the breach.
- The categories of personal data affected.

- Approximate number of data subjects affected.
- Name and contact details of the DPO/PO.
- Consequences of the breach.
- Any measures taken to address the breach.
- Any information relating to the data breach.

The DPO/PO notifies the supervisory authority. Contact details for the supervisory authority are recorded and a log of breach is maintained as per the incident breach management policy. In the event the supervisory authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

The breach notification is made by email, phone call, etc. A confirmation of receipt of this information is made by email, phone call, etc.

5.2.2 Data Subject Notification

If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Peoplesafe notifies the data subjects affected immediately with the DPO/PO recommendations.

The notification to the data subject describes the breach in clear and plain language, in addition to information specified in the previous section.

Peoplesafe takes measures to render the personal data unusable to any person who is not authorised to access it.

The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur by ensuring data is up to date or disposed of securely where no longer necessary for the effective management of users Personal safety.

If the breach affects a high volume of data subjects and personal data records, Peoplesafe makes a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder Peoplesafe's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner.

If Peoplesafe has not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, Peoplesafe will communicate the data breach to the data subject by email communication with the Account Admin for the affected data subjects.

Peoplesafe documents any personal data breach, incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

6. Data Protection Impact Assessment (DPIA)

6.1 Policy

All projects / new initiatives that involve processing personal data, or any activities (both internal and external) that affect the processing of personal data and impact the privacy of data subjects are within the scope of this procedure and will be subject to a data protection impact assessment (DPIA).

The DPO/PO is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA.

The top management and the IS group are responsible for checking appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.

6.2 Procedure

All identified projects are considered for the need for a DPIA at the start of each project, assessing the project and type of personal data involved, or processing activity, against the screening questions set out in the internal data control/mapping document.

Using the criteria below, following the likelihood and impact matrix, Peoplesafe defines the risks to rights and freedoms of data subjects.

Likelihood and impact matrix:

Likelihood					
	3	0	3	6	9
	2	0	2	4	6
	1	0	1	2	3
		0	1	2	3
				Impact	

Risks to rights and freedoms of data subjects:

Risk Level	From	To	GDPR Assessment
High	6	9	Highest unacceptable risk
Medium	3	5	Unacceptable risk
Low	1	2	Acceptable risk
Zero	0	0	No risk

6.2.1 Data Processing (Data Flow)

Peoplesafe records key information about all personal data processed for each project and process in the data processing control & mapping document. This includes a description of the processing and purposes; legitimate interests pursued by the controller; an assessment of the necessity and proportionality of the processing; an assessment of the risks to the rights and freedoms of data subjects (as per the matrix and risk level).

Peoplesafe establishes on what lawful basis the data is being processed and its appropriate retention period.

Peoplesafe identifies the category of data processed, whether it is personal, special or that of a child.

Peoplesafe identifies who has access to the data (individuals, teams, third-parties or data processor) or who are involved in the processing of personal data, or processing activity, recording the geographic location of where the processing takes place.

6.2.2 Privacy Risks

Peoplesafe assesses the privacy risks for each process activity:

- Identifying and describing the privacy risk associated to that process activity
- Using the likelihood criteria (1=low, 2-medium and 3=high), scoring the likelihood of the risk occurring
- Using the impact criteria (0=zero impact, 1=low, 2=medium and 3=high) of the risk should it occur
- Producing a calculated risk, identifying the risk to the rights and freedoms of data subjects.

In assessing the privacy risks, Peoplesafe considers: risks to the rights and freedoms of natural persons resulting from the processing of personal data; risks to the business (including reputational damage); and its objectives and obligations (both regulatory and contractual).

Peoplesafe identifies solutions to privacy risks, assigns a risk treatment and sets a target date for completion. Peoplesafe also prioritises analysed risks for risk treatment based on the above risk level criteria.

6.2.3 Prior Consultation (Article 36, GDPR)

Where the DPIA identifies that processing of personal data will result in high risk to the data subject, in the absence of risk mitigating measures and controls, Peoplesafe consults with the supervisory authority, using the following method.

- When Peoplesafe requests consultation from the supervisory authority it provides the following information:
- Detail of the responsibilities of Peoplesafe (Data Processor), and the data controller involved in the processing;
- Purpose of the intended processing;
- Detail of any/all measures and controls in place/provided to protect the rights and freedoms of the data subject(s);
- Contact details of the DPO/PO
- A copy of the data protection impact assessment; and any other information requested by the supervisory authority.

7. Retention of Records

All company records, whether analogue or digital, are subject to the retention requirements of this procedure.

This policy should be read in line with the Data disposal and retention policy as described in Peoplesafe It Cyber Security Policy.

- Asset owners are/responsible for ensuring that all personal data is collected, retained and destroyed in line with the requirements of the GDPR.
- The Finance Director is responsible for retention of financial (accounting, tax) related records.
- The HR Manager is responsible for retention of all HR records.

The Health & Safety representative is responsible for retention of all Health and Safety records.

- The Company Secretary is responsible for retention of all other statutory and regulatory records.
- The DPO/PO is responsible for storage of data in line with this procedure.
- The IT Director is responsible for the storage of infrastructure.
- The managers are responsible for ensuring that retained records are included in business continuity and disaster recovery plans.

The managers are responsible for ensuring that retained records are included in business continuity and disaster recovery plans.

7.1 Policy

The required retention periods, by record type, are recorded in the data control and mapping document. A companywide general retention period document is also available in QMS.

7.2 Procedure

Peoplesafe shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

Peoplesafe may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in Restricted Data – Disposal Policy along with the criteria used to determine this period including any statutory obligations Peoplesafe has to retain the data.

Under the agreement, personal data must be disposed of securely processed in an appropriate manner to maintain security, thereby protecting the “rights and freedoms” of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure. Please refer to Peoplesafe IT Cyber Security Policy.

Personal data should be reviewed periodically to check that they are accurate and up to date and to determine whether retention is still necessary.

Adequate measures should be taken to safeguard data so as to prevent loss, destruction or unauthorised disclosure. The more sensitive the data, the greater the measure that need to be taken.

Sub Contract Processing

All external suppliers that process personal data on behalf of Peoplesafe are within the scope of this procedure.

8.1 Policy

The DPO/PO is responsible for approving the selection of all sub-contracted processors of personal data in line with the requirements of this procedure.

The owners of third-party relationships are responsible for ensuring that all external data processing is contracted out in line with this procedure.

The QMS team is responsible for carrying out regular audits of third-party compliance.

8.2 Procedure

Peoplesafe selects only suppliers that can provide technical, physical and organisational security that meet company's requirements in terms of all the personal data they will process on company's behalf. Peoplesafe will ensure that all security arrangements are outlined in the contract with the external processor.

Suppliers from outside the EU will only be selected under the conditions - if the supplier or the state in which it resides has been positively identified in an adequacy decision by the EU Commission; or where there are legally binding corporate rules, and organisational and technical safeguards, established between Peoplesafe and the supplier to secure the rights and freedoms of data subjects at least equal to those afforded within the EU; or where the arrangement has been approved by the supervisory authority.

An information security risk assessment, taking into account the information security controls of ISO 27001

If the DPO/PO considers it necessary because of the nature of the personal data to be processed or because of the particular circumstances of the processing, an audit of the supplier's security arrangements against the requirements of ISO 27001 may be conducted before entering into the contract.

Peoplesafe requires a written agreement to provide the service as specified and requires the supplier to provide appropriate security for the personal data it will process.

Contracts with second-level subcontractors will only be approved if they require the subcontractors to comply with at least the same security and other provisions as the primary subcontracting organisation (the supplier) if they specify that, when the contract is terminated, related personal data will either be destroyed or returned to Peoplesafe, and so on down the chain of sub-contracting.

Review

The policy will be reviewed periodically, at least once a year to take account of changes in the law and guidance issued by the Information Commissioner.

Appendices

1. A copy of the certificate of Peoplesafe registration with the Information Commissioner can be obtained from Peoplesafe
2. Guidance notes

Appendix – Guidance

Data protection legislation does not guarantee personal privacy at all costs, but aims to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information. It applies to some paper records as well as computer records.

This short checklist will help you comply with the GDPR. Being able to answer 'yes' to every question does not guarantee compliance, and you may need more advice in particular areas, but it should mean that you are heading in the right direction.

- Do I really need this information about an individual? Do I know what I'm going to use it for?
- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- If I'm asked to pass on personal information, would the people about whom I hold information expect me to do this?
- Am I satisfied the information is being held securely, whether it's on paper or on computer? And what about my website? Is it secure?
- Is access to personal information limited to those with a strict need to know?
- Am I sure the personal information is accurate and up to date?
- Do I delete or destroy personal information as soon as I have no more need for it?