REDINGTON

DATA PRIVACY POLICY

Redington

03 June 2019

QAS Institute and Faculty of Actuaries Quality Assurance Scheme

For Internal Use Only

TABLE OF CONTENTS

Document Control

This policy is issued for internal use only. Information contained herein must not be reproduced in whole, or in part, not communicated to any third party except with the written authorisation of the author.

All hard copies of this document should be shredded after use.

Date	Author	Role	Version	Details
13 Jun 18	Jake Barker	Information Security Officer	0.1	Initial Draft
03 June 19	Ineshan Reddy	Information Security Officer & DPO	0.2	Small update

INTRODUCTION

This document sets out how Redington handle the personal data of our customers, suppliers, employees, workers and other third parties.

This policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, clients or supplier contacts, or any other Data Subject.

It sets out the standard what Redington expects from its employees, in order for the company to comply with UK and international law.

Roles and Responsibilities

Role	Responsibility
The Board	Overall responsibility for Data Protection
Information Security Officer (ISO) and Data Protection Officer (DPO)	Deferred responsibility for Data Protection from the board. › Governance, compliance, risk, and policy › Client assurance › Internal advisory and assurance › Training, education, and awareness
Head of Compliance	› Compliance oversight on Data Protection › Escalation of Data Protection risks

Scope

Everyone at Redington is responsible for protecting the confidentiality and integrity of data. Under GDPR, the company is exposed to fines of up to £18m or 4% of annual turnover (whichever is higher).

Consultation

The Information Security Officer & DPO should be consulted for the following:

- Questions about the six lawful basis to process personal data
- The capture of explicit consent
- The drafting of privacy notices or fair processing notices
- Data retention periods
- Information Security measures
- Data Breaches
- Transferring data outside of the EEA
- Subject Access Requests (SARs)

- New data processing activities or changes to data processing activities
- Automated processing of data or automated decision-making
- Direct marketing activities using the legitimate interest basis
- Contracts or other areas that share personal data with third parties

PERSONAL DATA PROTECTION PRINCIPLES

Redington adheres to the GDPR principles relating to the processing of personal data, which require personal data to be:

1. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
2. Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
4. Accurate and where necessary kept up to date (Accuracy).
5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
7. Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
8. Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

LAWFULNESS, FAIRNESS, AND TRANSPARENCY

Lawfulness and Fairness

Personal data must be processed lawfully, fairly, and in a transparent manner.

Processing must meet one of the six requirements below:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

d) **Vital interests:** the processing is necessary to protect someone's life.

e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Consent

An individual or client consents to the processing of their personal data if they indicate agreement clearly either by a statement or a positive action.

a) Omission, silence, inactivity, or even pre-ticked boxes are not sufficient

b) Individuals or clients must be able to easily withdraw consent to processing at any time and withdrawal should be prompt

c) Consent must be refreshed if data is going to be processed for a different or incompatible purpose which was not disclosed when consent was first given

d) Unless we can rely on another legal basis, consent is usually required for processing sensitive personal data, automated decision-making, and data transfer to third parties or outside the EEA

e) Records must be kept of consent by the department that obtained the consent

Transparency (notifying data subjects)

We must provide detailed, specific information to individuals and clients, depending on whether the information was collected directly from them or elsewhere. This is currently achieved through our privacy notice.

Whenever we collect personal data, we must provide the individual or client with all the information required by GDPR:

a) Identity of the Data Controller
b) How and why we will use the data
c) How we will process the data
d) To whom we will disclose the data
e) How will protect and retain the data

All personal data collected through third parties should also meet the above requirements.

LIMITATIONS

Purpose Limitation

Personal data must be collected only for specified, explicit, and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Data Minimisation

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

a) Employees can only process personal data when their role requires it
b) Employees can only collect personal data that is required for their role and may not collect excessive data
c) Employees must ensure that when personal data is deleted or anonymised when no longer required.

Accuracy

Personal data must be accurate and, where necessary, kept up to date. It should be corrected or deleted without delay once the inaccuracy is known.

Storage Limitation

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which Redington processed the data.

Redington will delete all personal data held after 7 years, unless required for ongoing purpose or legal reasons. Clients and individuals are informed of this in the Redington Privacy Policy.

Any data should be deleted by the IT Delivery Team, to ensure that it is properly destroyed. If third parties are required to delete data held, they will be contacted by the Compliance team.

SECURITY, INTEGRITY, AND CONFIDENTIALITY

Protecting Personal Data

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Redington will:

- Maintain information security by protecting the confidentiality, integrity, and availability of personal data:
  - *Confidentiality*: only accessible to those who have a need to know and are authorised
  - *Integrity*: personal data is accurate and suitable for purpose
  - *Availability*: able to access personal data when required to
- Develop, implement, and maintain safeguards appropriate to our size, scope, and business, our available resources, identified risks, and the amount of personal data we own or maintain on behalf of others.
- Regularly evaluate and test the effectiveness of our information security
- Implement reasonable and appropriate measures to prevent unlawful or unauthorised processing of personal data
- Implement reasonable and appropriate measures to prevent the accidental loss of, or damage to, personal data
- Exercise particular care in protecting sensitive personal data, which covers:
  d) race
  e) ethnic origin
  f) politics
  g) religion
  h) trade union membership
  i) genetics
  j) biometrics
  k) health
  l) sex life
  m) sexual orientation

Reporting a data breach

The Information Security Officer & DPO should be informed if a data breach has occurred. Employees should not attempt to investigate the matter themselves, or alter the data affected. The Information Security Officer & DPO will inform ICO within 72 hours and involve other organisations, such as the police, if required.

Data breaches include:

a) Access by an unauthorised third party
b) Deliberate or accidental action (or inaction) by a controller or processor
c) Sending personal data to an incorrect recipient
d) Physical data assets containing personal data being lost or stolen
e) Alteration of personal data without permission
f) Loss of availability of personal data

The Redington Data Breach Policy covers the process for data breaches.

TRANSFER OUTSIDE THE EEA

The GDPR restricts data transfers outside of the EEA in order to ensure that the level of data protection afforded to individuals is not undermined.

Data is transferred when it is transmitted to, sent to, viewed in, or accessed in a different country.

Redington will only send data outside of the EEA in exceptional circumstances. In these cases, the following must be satisfied:

a) The European commission has issued a decision confirming that the country involved has an adequate level of protection for the data subjects' rights and freedoms.
b) Appropriate safeguards are in place, such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification method.
c) The data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or
d) The transfer is necessary for one of the other reasons set out in the GDPR, including the performance of a contract, reasons of public interest, exercise or defend legal claims to protect the vital interest of the data subject. In some limited cases, legitimate interest may apply.

DATA SUBJECT'S RIGHTS AND REQUESTS

Data subjects have rights when it comes to handling their personal data. Their rights are:

a) Withdraw consent to processing at any time;
b) Receive certain information about the data controller's processing activities;
c) Request access to their personal data that Redington holds;
d) Prevent our use of their personal data for direct marketing purposes;
e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed, or to rectify inaccurate data, or to complete incomplete data;
f) restrict processing in specific circumstances;
g) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
h) request a copy of an agreement under which personal data is transferred outside of the EEA;
i) object to decisions based solely on automated processing, including profiling (ADM);
j) prevent processing that is likely to cause damage or distress to the data subject or anyone else;
k) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
l) make a complaint to the supervisory authority; and
m) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

The Information Security Officer & DPO will deal with all Subject Access Requests (SARs). They will verify the identity of the data subject and ensure the SAR complies with the GDPR, including the 30-day timeframe.

The process for SARs is detailed in the Redington SAR Process document.

ACCOUNTABILITY

Data controllers within Redington must implement appropriate technical and organisational measures to ensure compliance with data protection principles. The data controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

Redington have controls in place to ensure and to document GDPR compliance, including:

a) implementing privacy by design when processing personal data and completing Data Protection Impact Assessments (DPIAs) where processing presents a high risk to rights and freedoms of data subjects;
b) integrating data protection into internal documents including this privacy standard, related policies, privacy guidelines, privacy notices or fair processing notices;
c) regularly training company personnel on the GDPR, this privacy standard, related policies and privacy guidelines and data protection matters including, for example, data subject's rights, consent, legal basis, DPIA and personal data breaches; and
d) Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

Record Keeping

The GDPR requires Redington to keep full and accurate records of all our data processing activities.

Where consent is obtained, this must be documented.

These records should include:

a) the name and contact details of the data controller and Information Security Officer & DPO;
b) clear descriptions of the personal data types;
c) data subject types;
d) personal data storage locations;
e) personal data transfers;
f) the retention period; and
g) a description of the information security measures in place

Training and Audit

Redington conducts GDPR training through CybSafe. The Information Security Officer & DPO is responsible for training and will keep a record of those who have completed training.

Privacy by Design

Redington are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisation measures (like Pseudonymisation).

Data Protection Impact Assessment (DPIA)

DPIAs must be conducted when implementing major system or business change programs that involve the processing of personal data, including:

a) The use of new technologies (programs, systems, or processes), or changing technologies;
b) Automated processing, including profiling and automated decision-making
c) Large scale processing of sensitive data; and
d) Large scale, systematic monitoring of a publicly accessible area

A DPIA must include:

a) A description of the processing, its purposes, and the data controller's legitimate interests if appropriate;
b) An assessment of the necessity and proportionality of the processing in relation to its purpose;
c) An assessment of the risk to individuals; and
d) The risk mitigation measures in place and demonstration of compliance.

Automated Processing and Automated Decision-Making (ADM)

ADM is prohibited when a decision has a legal or otherwise significant effect on an individual, unless:

a) A data subject has explicitly consented;
b) The processing is authorised by law; or
c) The processing is necessary for the performance of or entering into a contract.

If a decision is to be solely based on Automated Processing, then data subjects must be informed when you first communicate with them of their right to object. The right must be explicitly brought to their attention and presented clearly and separately from other information.

Further to this:

a) Suitable measures must be put in place to safeguard their rights, freedoms, and legitimate interests;
b) They must be informed the logic involved in the decision-making or profiling;
c) They must be informed of the significance, and envisaged consequences; and
d) They must be given the right to request human intervention, express their point of view, or challenge the decision.

A DPIA must always be carried out before any ADM.

Direct Marketing

Redington is subject to certain rules and privacy laws when marketing to our customers.

- A data subject's prior consent is required for electronic direct marketing.
- Clients will most likely be contacted under the consent or contractual basis.
- Direct marketing may be used under legitimate interest basis, at the discretion of the Head of Marketing.

Sharing Personal Data

Personal data should only be shared internally where the recipient has a job-related need to know the information.

Most client contracts forbid the sharing of client personal data with third parties. Redington will not share personal data with third parties, unless certain safeguards and contractual agreements have been put in place.

If personal data absolutely must be shared with a third party, the following safeguards should be employed:

a) The third party must have a need to know the information for the purposes of providing the contracted services;
b) Sharing the personal data complies with the privacy notice provided to the data subject or client and, if required, the data subject or client's consent has been obtained
c) The third party has agreed to comply with the required data security standards, polices, and procedures and put adequate security measures in place;
d) The transfer complies with any applicable cross border transfer restrictions; and
e) A fully executed written contract that contains GDPR approved third party clauses has been obtained.