Data Protection Policy

Key points to remember……

- **This Data Protection Policy (Policy) sets out how Rentokil Initial plc and its relevant subsidiaries (we, our, us, RI) handle the Personal Data of our customers, suppliers, employees, workers and other third parties.**
- **This Policy applies to employees, consultants, contractors, secondees, temporary workers and other staff who work for or with us (you, your) and who are involved in or who have access to Personal Data.**
- **Any breach of this Policy may result in a fine or claim against RI and reputational damage and therefore may result in disciplinary action.**
- **Personal Data should be:**
    - **Used lawfully, fairly and in a transparent way;**
    - **Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;**
    - **Relevant to the purposes we have told you about and limited only to those purposes;**
    - **Accurate and kept up to date;**
    - **Kept only as long as necessary for the purposes we have told you about; and**
    - **Kept securely.**
- **You must immediately forward any Data Subject Request you receive to the relevant Local Privacy Officer (LPO) or the Data Protection Officer.**
- **If you know or suspect that a potential Personal Data Breach has occurred, do not attempt to notify the Personal Data Breach yourself - please notify your LPO and the DPO immediately.**
- **If you have a complaint and/or want to get more details about this policy please contact your Local Privacy Officer or the Group Data Protection Officer at dpo@rentokil-initial.com.**
-

PURPOSE AND SCOPE

Rentokil Initial plc, and its relevant subsidiaries (we, our, us, RI) is committed to protecting the privacy of colleagues (including applicants to become colleagues), customers, and other individuals' personal data. RI has implemented a privacy program to establish and maintain high standards for collecting, creating, using, disclosing, storing, securing, accessing, transferring, or otherwise processing personal data.

RI shall comply with applicable personal data protection and privacy laws and requirements within the countries in which we operate.

Where applicable personal data protection and privacy laws require a higher standard of protection for personal data than presented in this global privacy policy, the requirements of applicable personal data protection law shall prevail. Where applicable personal data protection and privacy laws establish a lower standard of protection for personal data than presented in this global privacy policy, the requirements of this global privacy policy shall prevail.

If there are applicable local laws, this Policy may be adapted to include the local requirements with approval from the Group Data Protection & Legal Compliance Officer at dpo@rentokil-initial.com

If any local Policy is created to meet local laws, it will be the responsibility of the Regional Managing Director who can delegate to a direct report at their election, or the country LPO to own, manage and update that Policy.

This Policy applies to all RI colleagues (you, your, we) who are involved in or who have access to personal data. If you are unclear about the Policy or how it impacts your role you should speak to your manager, your Local Privacy Officer (LPO) or the Group Data Protection & Legal Compliance Officer (DPO) (dpo@rentokil-initial.com). Additionally, all business units must ensure they have appropriate local standards and procedures in place to comply with this policy and applicable data privacy legislation in their jurisdiction.

Data Protection Policy

Breaches of this policy will be taken seriously and may result in disciplinary action, up to and including termination.

COMMUNICATION AND RESPONSIBILITIES

All colleagues are responsible for:

- Reading and complying with this Policy and related policies, along with related documents/guidelines that may be developed and maintained to implement the requirements of this Policy.
- Reporting violations of this Policy.

Managers and Team Leaders are additionally responsible for:

- Ensuring all reporting colleagues understand the requirements of this Policy.
- Ensuring appropriate safeguards are in place to protect personal data.
- Providing all necessary training and/or guidance to assist with the implementation process, and for monitoring compliance with this Policy

DATA PROTECTION PRINCIPLES

RI is committed to processing data in accordance with its responsibility under privacy legislation.

Processing your personal data, and the personal data of all colleagues (including applicants to become colleagues), customers, and other individuals will:

a. **BE FAIR:**

Personal data shall only be processed for a specific, explicit, and legitimate purpose(s). Any subsequent processing shall be compatible with such purpose(s).

Personal data shall only be processed where one of the following is met:

1. The data subject has given their consent
2. In life-or-death situations where there is no time to gain consent
3. To meet our legal compliance obligations
4. When processing is necessary to perform our contractual obligations (e.g., providing a service)
5. To operate our business, for example:
    - to send important notices such as communications about changes to our terms and conditions and policies
    - to provide important real-time information about products or services
    - to send information requested by the data subject or to respond to their enquiries
    - to develop, deliver and improve our goods or services
    - for internal purposes for research, analysis, testing, monitoring, customer communication, risk management and administrative purposes
    - for direct marketing or determining the effectiveness of promotional campaigns and ads
    - for data analytics or identifying usage trends
    - to protect and defend our rights or our property

Rentokil Initial

Data Protection Policy

Personal data about colleagues or applicants to become colleagues may be processed for the purposes set out in the RI Employee Data Privacy Notice or RI Careers Data Privacy Notice.

Personal data about customers or prospective customers may be processed for the purposes set out in the RI Privacy Notice.

b. BE LIMITED IN USE:

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Accessing and processing personal data is limited to required job duties.

c. BE PROPORTIONAL:

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

d. MAINTAIN DATA INTEGRITY:

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is accurate, having regard to the purposes for which it is processed, erased or rectified.

e. FOLLOW A DATA LIFECYCLE AND RETENTION PERIOD:

Personal data shall be kept for no longer than is necessary for the purposes for which the personal data is processed.

You must keep and maintain accurate corporate records reflecting our processing in accordance with RI's Document and Data Retention Policy.

Local statutory retention policies must always be followed. Contact your LPO for questions about your applicable local Document and Data Retention Policy.

f. ENSURE DATA SECURITY:

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This includes ensuring any third-party data processor also has the appropriate levels of security.

Sensitive personal data is handled with extra security. In many jurisdictions it requires documentation of the lawful reason for processing. Ask your local LPO or the Group Data Protection & Legal Compliance Officer if you have questions.

Refer to the RI Global Information Security Policy.

g. RESPECT THE RIGHTS OF DATA SUBJECT RIGHTS:

Data subject rights shall be processed in a manner that respects individuals' rights under applicable data protection legislation.

Individual rights include:

- the right to be informed about the collection and the use of their personal data (transparency)
- the right to access personal data
- the right to have inaccurate personal data rectified, or completed if it is incomplete

- the right to erasure (to be forgotten) in certain circumstances
- the right to restrict processing in certain circumstances
- the right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services
- the right to object to processing, sharing or selling personal data in certain circumstances
- rights in relation to automated decision making and profiling
- the right to withdraw consent at any time (where relevant)
- the right to complain to a regulator

If an individual contacts RI and requests to exercise their rights, inform your LPO or the Group Data Protection & Legal Compliance Officer as soon as possible as there are statutory time limits in which we have to respond to the data subject.

h. <u>BE REPORTED IN THE EVENT OF A DATA BREACH:</u>

Data protection legislation requires data controllers in certain instances to notify personal data breaches to the applicable data protection authority and the data subject.

Examples of personal data breaches may include:

- Human error, for example an email attachment containing personal data being sent to the incorrect recipient or records being deleted accidentally
- Sharing of passwords or other credentials with third parties
- Controlled documents being left unattended to be copied, read or photographed by an unauthorised person
- Loss or theft of a physical file or electronic device containing personal data
- Opening or clicking a link within a malicious email which contains malware or viruses
- A ransomware attack whereby access to systems or records containing personal data is disabled or encrypted
- A cybersecurity attack whereby personal data is accessed, altered, deleted and/or disclosed by the attacker

RI has procedures to deal with any suspected personal data breach and will notify data subjects or any applicable data protection authority where we are legally required to do so. If you know or suspect that a personal data breach has occurred, <u>do not attempt to notify those impacted by the data breach yourself.</u>

ANY INDIVIDUAL NOTICING AN ACTUAL OR SUSPECTED PERSONAL DATA BREACH MUST IMMEDIATELY REPORT IT TO THE LOCAL IT SERVICE DESK EITHER BY PHONE, BY THEIR IT SUPPORT SYSTEM OR VIA THEIR MANAGER. The incident description should make it clear that it is a potential personal data incident, so that it can be promptly directed to the privacy team.

i. <u>BE TRANSFERRED LAWFULLY:</u>

Data protection legislation may restrict data transfers outside of a political or geographical region. For example, data transferred outside of the European Economic Area requires the third country to have adequate levels of protection for data subjects or other mechanisms such as standard contractual clauses executed to govern the

transfer. Ask your local LPO or the Group Data Protection & Legal Compliance Officer if you have questions regarding the transfer of personal data.

DEFINITIONS

Data Controller - the person or company that determines the purposes and means of the processing of personal data. RI and its affiliates or subsidiaries are usually the data controller for data we collect, create, use, disclose, store, secure, access and transfer.

Data Protection Impact Assessments (DPIA) - Also known as privacy impact assessments, are tools and assessments used to identify and reduce risks of a data processing activity. DPIAs should be conducted for all major system or business change programs involving the processing of personal data.

Data Processors – an entity that processes personal data on behalf of a data controller. Vendors and suppliers are generally categorized as data processors.

Data Protection Legislation - all legislation and regulatory requirements relating to the use of personal data in the applicable jurisdiction.

Data Subject – the identified person or household whom personal data relates to.

Personal Data - information that can be related to an individual. Personal data can be factual (names, addresses, government issued numbers, video, etc.) or it can be an opinion.

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.

Processing or Process - any activity that involves use of personal data. This includes obtaining, recording or holding the data; carrying out any operation or set of operations on the data by automated means or manually, including organising, amending, retrieving, accessing, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive Personal Data - information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sexual life and / or orientation, biometric or genetic data, financial account and government identification numbers.

RELATED POLICIES AND NOTICES

- Data Privacy Notices
- RI Global Information Security Policy
- Document and Data Retention Policy

REVISIONS TO THE POLICY

Date	Changes	Policy Owner	Review Frequency
May 2023	Substantial – all sections revised to reflect a global policy	Group Data Protection & Legal Compliance Officer	Annually