Group Policy Statement

Data Privacy Policy

Royal Mail Group (RMG) respects the privacy of all its colleagues and customers in relation to any personal data it collects, stores and processes about them. We accept our responsibility to ensure that all such personal data is managed in line with all applicable data protection and privacy laws. This policy sets out the steps our people must take to do this.

We will:

- Only use personal data for specified and lawful purposes and in line with our published Privacy Notice[1] and Employee Privacy Notice[2].
- Apply Privacy by Design and complete a Data Privacy Impact Assessment (DPIA) for all projects which introduce a new system, process (including analytics), product (including Artificial Intelligence [AI]) or use personal data for a new purpose, including where third parties access RMG systems or personal data, in line with RMG guidance[12].
- Classify[3] and protect any personal data RMG holds based on its volume, importance and sensitivity to the business and individuals, applying additional protection as required to special category (see Appropriate Policy Document[4]), other sensitive personal data (e.g., children or vulnerable people), payment card data (PCI Standard[5]). Please refer to the Personal Data Use Standard[9] for more information.
- Ensure personal data is kept accurate and up to date, deleted and disposed of carefully and only retained for the time period set out in our Corporate Retention Schedule[6].
- Complete data protection and information security training promptly as required.
- Report any actual or suspected personal data breaches to the IT Helpdesk as soon as possible.
- Follow all the additional requirements regarding the protection of personal data including any individual responsibilities of usage of RMG devices which is outlined in the Information Security Policy[7] and Acceptable Use Policy[8].
- Ensure the necessary due diligence is conducted and data sharing, and transfer requirements applied when using a third-party supplier to process personal data on RMGs behalf, or when we transfer personal data outside the UK.
- Maintain a central record of all personal data processing activities by the DPO team and manage risks in accordance with the risk management framework.

26th June 2024

Policy Owner: Director of Privacy and DPO

Where to go for help

This policy is supported with the following documents:

1. Privacy Notice
2. People Privacy Notice
3. Information Classification Standard (Internal only)
4. Appropriate Policy Document (Internal only)
7. Information Security Policy (Internal only)
8. Acceptable Use Policy (Internal only)
9. Personal Data Use Standard (Internal only)
10. How to detect and report incidents (Internal only)

5. PCI Standard (Internal only)
6. Corporate Retention Schedule (Internal only)
11. Privacy Risk Handbook (Internal only)
12. Think Secure – DPIA Guidance (Internal only)

Getting help with this Policy

If you have any concerns with this policy, please contact irgt@royalmail.com.

Who does this Policy apply to?

This policy applies to all employees, workers, consultants, self-employed contractors, casuals, and agency workers. engaged by International Distribution Services plc, Royal Mail Group Limited and their wholly or majority owned subsidiary companies and joint ventures, excluding General Logistic Systems B.V group, which maintains its own compliance policies and procedures which are aligned with this policy.

Breach of this Policy

These Privacy Principles are mandatory. Any employee that fails to comply with this policy may be subject to conduct action up to and including dismissal. You may also commit a criminal offence if you deliberately access, disclose, or misuse personal data. This includes obtaining stolen marketing lists or taking customer or colleagues data for your own use. RMG employees have a legal obligation to formally report data incidents[10] which have led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. These could include Loss or theft of devices or data, including on USB drives or paper; Hacking or other forms of unauthorised access to a device, email account, or the network; Disclosing personal data to the wrong person, through wrongly addressed emails; Alteration or destruction of personal data without permission.