RMG00000091

Royal Mail Group

# Data Protection and Privacy Policy

Protecting our people and brand
Respecting privacy rights
Knowing how to do the right thing

Policy Owner: Director of Information Governance and DPO

Date: June 2020

RMG00000091

## Overview and Policy Statement

At Royal Mail Group (RMG) we are committed to protecting the confidential and personal details of our colleagues, customers and other individuals who trust us to handle their personal data safely and securely. We have a set of privacy principles which are based on data protection laws and everyone in RMG has a responsibility to handle data in line with these principles.

RMG respects the privacy of all its colleagues and customers and the confidentiality of any personal data it holds about them. This policy sets out what steps employees must take to ensure personal data is correctly handled. When handling personal data, the following Privacy Principles should be followed:

## Our Privacy Principles

**We must:**

- Only collect personal data that is relevant and used solely for the purpose in which it was collected and ensure that the data is processed under the right lawful basis.
- Only use personal data fairly and in accordance with the relevant published Privacy Notice and/or Employee Privacy Notice.
- Complete a Privacy Impact Assessment when undertaking a project for a new system, process or product that will involve processing personal data or when processing personal data for a new purpose.
- Keep personal data accurate and up to date and maintain a record of any changes.
- Make sure we keep personal data confidential and secure, and limit the people who can access it in line with the RMG Information Security Policy.
- Follow approved destruction and disposal processes as stipulated in the RMG Information Security Policy.
- Complete data security training promptly when requested.
- Report personal data breaches to the 24-hour IT Helpdesk on GRO as soon as possible.

**We must not:**

- Retain personal data for longer than necessary to achieve the business purpose or to meet minimum legal requirements. Check our Corporate Retention Schedule for guidance.
- Dispose of personal data carelessly.
- Discuss or disclose personal data to colleagues or anyone outside RMG unless there is a business reason to do so and this is relevant to the purpose for why it was collected.
- Transfer data outside the country in which it is collected, even within RMG, without advice from the legal team as there may be restrictions/requirements relating to the transfer.
- Use a third-party supplier to process personal data on our behalf without undertaking the necessary due diligence and ensuring there is a contract with an appropriate data processing and security clause in place. Seek guidance from Procurement if necessary.
- Deal with data protection issues and complaints without the proper advice. Pass data protection enquires to irgt@GRO.

RMG00000091

## Further information

### What is 'personal data'?

Personal data is any information that can be used to directly or indirectly identify a living individual. This can include name, email address, phone number, location data, financial data such as bank account or credit card information, CCTV footage, photographs or factors more specific to the physical or social identity of a person. It includes data held on our systems, in paper documents, emails, call recordings, mobiles or other storage media. It should be noted that information which doesn't immediately identify someone (e.g. address data) could still be considered personal data in Royal Mail's hands if it could identify a person when combined with other information we hold.

Certain data is especially sensitive and is known as "special category" data. Examples include information about someone's health, race, religious beliefs, political opinions, trade union membership, criminal offence or sexuality, and biometric or genetic data. There are extra requirements to ensure this data is handled in compliance with law, so if your job involves working with this information and you need advice please refer to our Guidance and ask the Information Rights and Governance team.

## Further guidance and documents

Corporate Retention Schedule
Privacy Notice
Privacy Impact Assessment
RMG Information Security Policy
RMG Information Security Classification Policy
Authority to Procure, Requisition and Pay Policy
Special Category Data – Appropriate Policy Document
ISS03 — Information Security — Data Backup and Restoration Standard
ISS04 - Information Security - Asset Management Standard
ISS05 - Information Security - Classification Standard
ISS06 - Information Security - Incident Management Standard

## Reporting Concerns

### If you see something, say something

Everyone should be able to raise concerns without fear of retaliation.

You can talk to your line manager or you can Speak Up by calling the confidential helpline on GRO GRO or using the on-line web-based service at www.intouchfeedback.com/royalmail. We will take action.

## Scope of Policy

This Policy applies to Royal Mail Limited and its wholly or majority owned subsidiary companies registered in the United Kingdom. Individuals include employees, casuals, agents, professional interims, agency workers, contract staff, consultants, officers and any other representative. This Policy does not form part of any employee's contract of employment and we may amend this policy at any time.

## Breach of this Policy

The Privacy Principles are mandatory. Any employee that fails to comply with this policy may be subject to disciplinary 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 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.

Where an employee discovers or suspects a personal data breach, this should be reported to the 24-hour IT Helpdesk on GRO as soon as possible.

## Getting help with this Policy

Please discuss any questions with your line manager or alternatively contact information.rights@ GRO .

Look at the security guidance from the Think Secure section on Royal Mail or contact **ThinkSecure@royalmail.com,** alternatively contact the Group Data Protection Officer.
For advice on this document or applicable standards, contact Group Compliance and Ethics.

- GRO or e-mail them at
- group.compliance@ GRO

RMG00000091

## Policy Governance

| | |
|---|---|
| Policy Reference number: | POD/COMP/POL/016 |
| Version Number: | 006.1 |
| Policy Owner: | Director of Information Governance and DPO |
| Policy Effective from: | June 2020 |
| Last Review Date: | May 2020 |
| Next Review Date: | May 2021 |
| Approved by: | Chief Risk and Governance Officer |
| Approval date: | June 2020 |

To request changes or updates to this document, e-mail: policy.governance@ GRO .

Please note this document is classified:

RMG – CONFIDENTIAL