# Gamma Group Data Protection Policy

**Gamma Communications plc ("Gamma")**

## Introduction

Data is an asset that allows technology companies such as Gamma to act. Data may relate to marketing forecasts, customer information, product usage statistics, technical designs and configurations, financial information, employee information or network availability metrics.

Gamma considers data protection to be a vital part of its internal controls and aims to implement relevant controls at the most appropriate level. With the intention to ensure data is available to those who need it, when they need it, to deliver against our objectives. While also ensuring those who do not need access are not able to use it inappropriately.

### Audience

Gamma Group

### Aims and goals

The aim of this policy is to ensure Gamma manages data we are responsible for in a consistent, legal, and appropriate way.

Our goals are to ensure Gamma data is:

a. Managed, processed and consumed in such a way as to ensure all data, not only personal data, is used correctly and in line with our risk appetite.

b. Protected in line with relevant, local regulation and legislation.

c. Protected in line with contractual obligations.

### Scope

All Gamma Group data

## Policy statements

1. Gamma will endeavour to make data available to Gamma employees who need it to be successful in their role.
2. Data will be protected consistently, based on a classification applied and potential risks faced.
3. Personal data, and sensitive personal data, will be managed in line with local legislation.
4. Gamma will be transparent with its customers regarding how their data is stored and processed, subject to any applicable local legal/security restrictions.
5. Gamma will risk assess third parties who have access to data Gamma is responsible for.

6. Whenever possible data protection controls will be systemised to ensure they are consistent and easily enforced by employees.
7. Gamma will ensure appropriate resources are made available to data protection and governance activities.

# Education & Training

Training will be role specific and managed through various learning and development initiatives.

# Roles and responsibilities

| Who | Key roles and responsibilities |
|---|---|
| **Group Subsidiary Managing Director** | Responsible for:<br>Maintaining access to a Data Protection Officer.<br>Providing appropriate resources are aligned to data protection activities, ensuring central reporting activity is completed as required. |
| **Data Protection Officer** | Responsible for representing the data protection interests of natural persons impacted by the relevant company and compliance with local personal data laws. |
| **Group Risk Management Team** | Responsible for ensure appropriating processes are in place to risk assess suppliers and third parties. |
| **Group Security Teams** | Responsible for outlining appropriate operational data protection controls. |
| **Group Architecture Review Board** | Responsible for ensuring data protection is considered in all relevant review activity. |
| **Group Business Continuity team** | Responsible for ensuring data is considered during business impact analysis activities. |
| **Data owners** | Responsible for ensuring the appropriate controls to ensure data is available and protected. |
| **Technology and Operations teams** | Responsible for the implementation of relevant data protection controls. |
| **All managers and employees** | Responsible for the appropriate control of data they manage on a day-to-day basis |

# Governance and reporting

Each country will have a local Data Protection Committee to drive risk reduction and data protection activities.

Local Data Protection Committees will report, on a quarterly basis, to the Gamma Group Data Protection Committee.

Data protection risks will be managed through the Gamma Group Risk Management Process.

Regulatory reporting will be managed in line with local regulatory and legal reporting processes.

Data incidents must be reported via the Security Incident Reporting process.

# Adoption

Those who believe there has been a breach of the data protection controls should raise their concerns as a security incident.

Employees who wilfully breach data protection controls may face disciplinary action.

Enforcement for suppliers should align with local legislation and where possible be stipulated in contractual clauses.

# Glossary

| Term | Definition |
|---|---|
| Personal data | Information related to natural persons who:<br>can be identified or who are identifiable, directly from the information in question; or<br>can be indirectly identified from that information in combination with other information. |
| Sensitive personal data | Special categories of personal data, being:<br>• racial or ethnic origin<br>• political opinions<br>• religious or philosophical beliefs<br>• membership of a trade union<br>• genetic data<br>• biometric data<br>• health<br>• sex life or sexual orientation<br>• criminal activity |

# Document Control

| | |
|---|---|
| Data Classification: | **Public - Published** |
| Document Ref: | G-RG-POL-003 |
| Document Owner: | John Murphy - Chief Operating Officer |
| Effective Date: | 31 January 2024 |
| Version: | 1.2 |
| Approved by: | The Gamma Board |