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
All managers and employees	Responsible for the appropriate control of data they manage on a day-to-day basis
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
Data owners	Responsible for ensuring the appropriate controls are in place and for making the data available as appropriate
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
Group Data Governance team	Responsible for the data privacy programme within Gamma Group
Group Risk Management Team	Responsible for ensuring appropriating processes are in place to risk assess suppliers and third parties
Group Security Teams	Responsible for outlining appropriate operational data protection controls, and deploying and monitoring the appropriate security toolset
Group Business Unit Managing Directors	Responsible for: Maintaining access to a Data Protection Officer. Providing appropriate resources are aligned to data protection activities, ensuring central reporting activity is completed as required.
Technology and Operations teams	Responsible for the implementation of relevant data protection controls.

Governance and reporting

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

Local Data Privacy Committees will report, on a quarterly basis, to the Gamma Group Data Privacy 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 Cyber Security Incident Response Procedure.

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: can be identified or who are identifiable, directly from the information in question; or can be indirectly identified from that information in combination with other information.
Sensitive personal data	Special categories of personal data, being: • racial or ethnic origin • political opinions • religious or philosophical beliefs • membership of a trade union • genetic data • biometric data • health • sex life or sexual orientation • criminal activity

Document Control

Data Classification:	**Public - Published**
Document Ref:	G-RG-POL-003
Document Owner:	Colin Lees, Chief Technology Officer
Effective Date:	06 February 2025
Version:	1.3
Approved by:	The Gamma Board