Data Protection Governance Directive

Document owner	Group Data Protection Officer
Approval	CEO and CFO
Initially adopted	3 September 2018
Date last approved	22 December 2025
Date of next review/approval	Q4 2026
Applicability	Group

Data Protection Governance Directive

1. Introduction

Viaplay Group processes personal data as part of its daily operations. The Group is committed to ensuring that all such processing is lawful, fair, secure, transparent and in line with applicable data protection legislation.

This Data Protection Governance Directive:

- sets out how data protection is organised and governed within Viaplay Group,
- defines roles and responsibilities,
- describes key control and operational layers, and
- complements the Viaplay Group Data Protection Policy and related guidelines.

All processing of personal data within Viaplay Group must be carried out in accordance with this Directive, the Data Protection Policy, applicable data protection legislation (including the GDPR), and relevant information security requirements.

1.1. Target group

This Directive applies to all Viaplay Group legal entities. The following groups are specifically required to read and understand this Directive and act in accordance with it:

Target Group	*Motivation*
Members of the Group Executive Team	Accountable for adherence to the principles in this Directive and for ensuring appropriate resources and support.
Members of Management Teams	Must build a data protection-aware culture and ensure sufficient resources within their respective areas to implement this Directive.
DPOs and Central Data Protection Team	Must know and apply this Directive and act in accordance with their defined roles and responsibilities.
All employees in Viaplay Group's Legal and Compliance functions	Must know and apply this Directive and other Group data protection policies and guidelines when providing legal advice and making decisions.

All managers are responsible for ensuring that relevant employees in their areas are familiar with this Directive and related instructions.

1.2. Definitions

Data controller – a natural person or legal entity that determines the purposes and means of personal data processing, either alone or jointly.

Data protection legislation – any applicable law or regulation concerning data privacy and protection that governs the processing of personal data, including without limitation

the Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement or such data (General Data Protection Regulation or "GDPR") or equivalent legislation (including judgments of any relevant court of law) and regulations relating to the processing of personal data, data privacy and data security, in each case as amended, extended or re-enacted from time to time and all orders, regulations, statutes, instruments or other subordinate legislation made thereunder in any relevant jurisdiction from time to time.

DPO – Data Protection Officer.

General Data Protection Regulation (GDPR) – EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Joint controller – two or more controllers that jointly determine the purposes and means of personal data processing.

Personal data – any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, genetic, mental, economic, cultural or social identity of that natural person.

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.

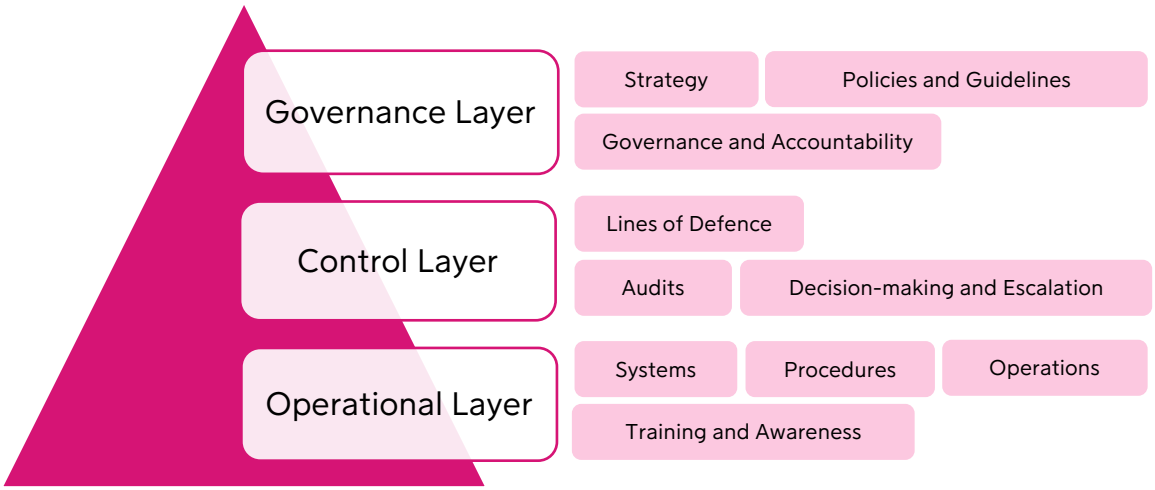
Processor – a natural person or legal entity that processes personal data on behalf of a data controller.

Processing – any operation or set of operations performed on personal data or sets of personal data, including by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Supervisory authority – an independent public authority monitoring the application of data protection legislation.

2. Data Protection Corporate Governance Model

Viaplay Group adopts a comprehensive data protection governance model, designed to operate across three interconnected layers: Governance Layer, Control Layer, and Operational Layer.



2.1. Governance Layer

2.1.1. Strategy and principles

Viaplay Group aims to be recognised as a reputable and trustworthy organisation that respects privacy and protects personal data. Accordingly, Viaplay Group must comply with the GDPR and all other applicable data protection legislation. Processing of personal data must follow the principles outlined in **Viaplay Group's Data Protection Group Policy**. All functions must integrate data protection considerations into their processes, systems, and projects.

2.1.2. Risks of non-compliance

Unlawful processing of personal data or a personal data breach may constitute non-compliance with data protection legislation. Consequences can include significant administrative fines, reputational damage, civil liability and possible criminal sanctions in some jurisdictions, loss of trust from critical stakeholders such as customers, employees, suppliers, and regulatory bodies.

Under the GDPR, infringements may lead to administrative fines of up to 20 000 000 EUR or up to 4% of Viaplay Group's total worldwide annual turnover of the preceding financial year, whichever is higher.

All functions must therefore treat data protection compliance as a core risk management area.

2.1.3. Roles and responsibilities

Data protection is a shared responsibility. The following roles are central to the governance model:

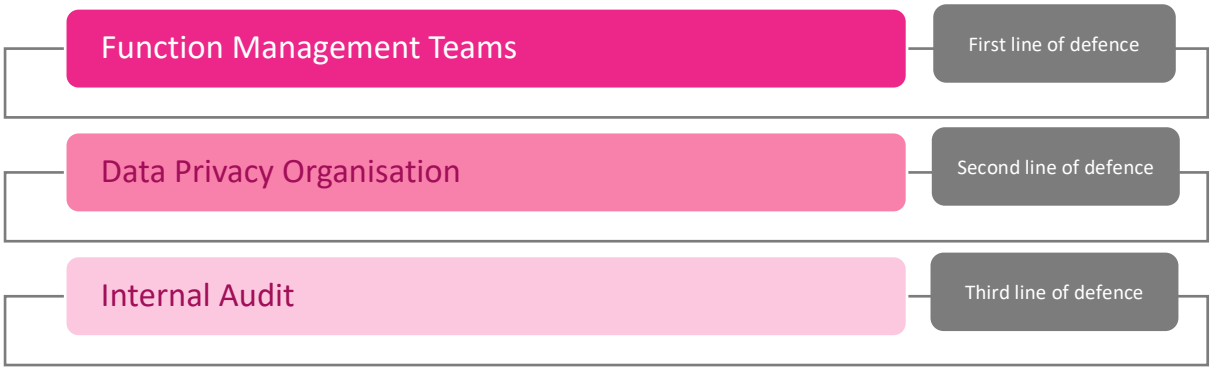
- **Group Data Protection Officer**
- **Local Data Protection Officers**

- **Central Data Protection Team**
- **Head of Group Compliance**
- **VP Group IT**
- **Function Management Teams**
- **Internal Audit**

These roles are further described in Section 2.2.

2.2. Control Layer – Three Lines of Defence

Viaplay Group\s data protection governance forms part of the overall Group governance and risk framework and is based on the three lines of defence model:



Viaplay Group uses a risk-based approach to data protection. Each function must:

- identify and manage privacy risks within its area,
- prioritise mitigation of high and immediate risks, and
- consider the nature, scope, context and purposes of its processing activities.

While the Data Privacy Organisation (led by the Group DPO) sets the overall framework, ownership of privacy risks lies with each function.

2.2.1. First line of defence – Function level

Function Management Teams are responsible for:

- implementing and adhering to Group data protection policies, directives and guidelines,
- integrating data protection principles into daily business processes,
- allocating appropriate resources to ensure compliance,
- implementing Viaplay Group's Compliance Management System (see Section 2.3.1) within their area,
- considering data protection as a standing agenda item in their management meetings, at least quarterly.

Data Protection Officers may escalate identified data protection risks and request decisions from the Function Management Teams, who must then decide on appropriate mitigating actions.

2.2.2. Second line of defence – Local and central level

Viaplay group may formally appoint local Data Protection Officers (Local DPOs) for entities where *any* of the following applies:

- large-scale regular and systematic monitoring of data subjects,
- large-scale processing of special categories of personal data as a core activity, or
- where local law requires the designation of a DPO.

Local DPOs respond to the competent Supervisory Authority and the data subjects, act as primary contact for data protection queries within their entity or market, and support the Group DPO in fulfilling the requirements of applicable data protection legislation.

Local DPOs responsibilities include:

- raising awareness and coordinating training on data protection (with support from the Group DPO);
- implementing Group data protection policies and guidelines locally;
- maintaining and approving records of processing activities and systems/assets the Compliance Management System;
- assisting with data subject requests from customers, business partners and employees;
- supporting the execution of Data Protection Impact Assessments;
- monitoring legislative changes and coordinating process adaptations in consultation with the Group DPO;
- coordinating audits of third-party processors when reasonably necessary and in cooperation with Viaplay Group's IT/Information Security teams;
- supporting negotiations of Data Processing Agreements with stakeholders and legal counsel;
- reporting and/or managing personal data breaches within their entity;
- submitting periodic Data Privacy Governance Report to the Group DPO, summarising activities, risks, incidents, breaches, mitigation and recommended improvements.

Group Data Protection Officer (Group DPO). The Group DPO is Viaplay Group's senior advisor on data protection matters and is responsible for maintaining Viaplay Group's data protection framework.

Group DPO responsibilities include:

- preparing, maintaining, and updating Group data protection policies, directives, guidelines and training activities;
- advising on and monitoring Group-wide compliance with data protection legislation, the Code of Conduct and Group policies;
- developing the annual data protection roadmap for Group and functions;
- establishing the yearly "governance wheel" of key GDPR topics to be reviewed, updated and maintained;
- acting as the main contact point for Local DPOs and providing advice, recommendations and updates on data protection issues;

- acting as principal contact point between Viaplay Group and supervisory authorities;
- updating the Central Data Protection Team on relevant data protection developments;
- compiling summaries of data protection reports and recommending follow-up actions;
- reporting data protection-related risks and issues to Viaplay Group's Audit Committee and Head of Risk Management.

Independence and authority are important for the fulfilment of the DPO role. To that end, the DPO:

- should perform his/her duties independently and without instruction regarding the exercise of these duties;
- can request and receive information regarding the processing of personal data without obstruction;
- should have direct access to the highest management level;
- may escalate issues to Internal Audit and to the Board of Directors of legal entities where necessary;
- is bound by confidentiality concerning the performance of his/her duties in accordance with the law;
- may not be instructed, dismissed or penalised by a data controller or data processor for exercising his/her duties;
- may document and escalate as necessary in the event of objections to his/her guidance;
- may exercise additional duties, but the organisation should ensure that such duties do not result in a conflict of interests;
- should receive sufficient resources and support to fulfil the role and maintain expert knowledge.

Central Data Protection Team. This team aims to synchronize the data protection work between the Data Privacy Organisation and Group IT/Information Security teams. The team also represents a "working committee" that advises on data protection issues affecting the whole Group. The team's objective is to ensure a uniform Group-wide approach to data protection. Members of the team include Group DPO, Head of Group Compliance, and VP Group IT. Representatives from other business areas and Group functions can be invited when necessary.

The Central Data Protection Team:

- makes decisions on data protection issues affecting multiple entities or the Group as a whole;
- bridges data protection and IT/Information Security responsibilities and allocates ownership;
- escalates major data protection issues, including those involving high risks and/or significant investments/costs.

VP Group IT is responsible for:

- aligning IT and information security initiatives with Group data protection policies and requirements;
- monitoring and supporting appropriate data protection setitngs and controls in Group systems/assets.

Head of Group Compliance is responsible for:

- assessing third-party management from a data protection perspective;
- coordinating with the Group DPO on data protection compliance priorities;
- monitoring regulatory initiatives and advising on necessary actions;
- supporting the internal distribution and communication of data protection processes.

2.2.3. Third line of defence – Central level

Internal Audit. The role of Viaplay Group's Internal Audit function is to provide independent assessment of the Group's governance, risk management, and internal control processes. This includes evaluating the adequacy and effectiveness of existing policies and procedures, and reviewing the systems established to ensure compliance with Viaplay Group's policies, procedures, laws and regulations. However, the Internal Audit process does not relieve departmental heads/managers of their responsibility for the maintenance and improvement of internal controls, and management of risks in their respective areas.

2.3. Operational Layer

The Operational Layer comprises the processes, procedures, systems and documentation that support day-to-day compliance with data protection requirements. Viaplay must implement appropriate technical and organisational measures to ensure and demonstrate compliance with the applicable data protection legislation.

2.3.1. Compliance Management System

Viaplay Group operates a **Compliance Management System** that is implemented centrally. The system contains information necessary to demonstrate compliance with data protection legislation and related compliance rules.

As part of this system, Viaplay Group uses OneTrust to document personal data processing across the organisation. It also contains data flows within and between Viaplay Group's companies, as well as with third parties. OneTrust is also a repository of information about data processors, the systems used to process data, the categories of personal data stored in these systems, and the designated retention periods for such data. OneTrust shall be regularly updated and supplemented as new processing activities, IT systems or services are developed or procured. Furthermore, Viaplay Group's Consent Management Platform for cookies and other tracking technologies on various platforms is implemented through OneTrust.

The Compliance Management System contains the following, among other things:

- information on how Viaplay Group's Data Protection Policy and other data protection guidelines are implemented;
- records of Viaplay Group's processing activities and assets;
- legitimate Interest Assessments;
- Data Protection Impact Assessments;
- records of Viaplay Group's vendors and data processors;
- information on data protection security requirements (see Viaplay Group's Information Security Group Directive);
- records of personal data breaches;
- records of Data Subject Rights Requests;
- annual Data Protection Governance Reports;

2.3.2. Relationships between Viaplay Group's legal entities

Data protection rights and obligations attach to **legal entities**, not to functional areas.

For each processing activity, a Viaplay Group legal entity must be identified as a **controller**, **joint controller**, or a **processo**r for another entity.

Where one Viaplay Group legal entity acts as controller and another as processor, a **data processing agreement (DPA)** must be in place, regardless of whether the entities are assigned to the same business area. Viaplay Group has an Intra-Group Data Processing and Transfer Agreement in place that covers transfer of data between legal entities.

Where two or more entities act as joint controllers, a **joint controller arrangement** must be in place defining responsibilities and compliance obligations under data protection legislation.

2.3.3. Tasks framework

Viaplay Group adopts a RACI approach where different stakeholders are assigned and made aware of their respective responsibilities. The following presents a high-level overview of the common privacy challenges addressed at Viaplay Group.

R - Responsible	**C** - Consulted	**A** - Accountable	**I** - Informed

Privacy Challenge	Team				
Owner	Data Privacy	Central Data Protection Team	Function	Internal Audit	Executive Leadership
Governance and Privacy Programme					
Governance model definition	R, A	I	I	I	I
Representation and Institutional Aspects					

Cooperation with supervisory authority (SA)	R, A	I		I	I
Point of contact with the SAs and data subjects	R, A	I	I	I	I
Data Inventory & Mapping					
Document personal data processing	C, I		R, A		
Create and maintain a RoPA	C, I		R, A	I	
Review processing to align with legal rules	R, A	C	I		
Data Protection Impact Assessments					
Develop and review DPIA methodology	R, A	I			
Conduct DPIA for high-risk activities	C		R, A		I
Data Security					
Develop policies for vendor security assessments	C	R, A	I		
Complete vendor security assessments	C	C	R, A		
Identify and document data breaches	C, I	I	R, A	I	I
Assess breach response procedure and notification	C	C	R, A	I	
Operational and IT changes implementation	C, I	A	R		
Awareness and Trainings					
Execution of training and awareness actions	R	C	I		I
Complete trainings	I		R		A

3. References

- Data Protection Policy
- Information Security Directive

4. Document History and Change Information

For more details of this Group Directive's document history and change information, see **Appendix 1**.

Appendix 1 – Document History and Change Information

Version	Revision Date	Change Information
1	2018-09-03	Initial Group Directive.
2	2019-12-13	Changes in roles & responsibilities due to internal reorganization. Changes in the governance structure and reporting set-up. Editorial changes.
3	2020-11-26	Deletion of core principles already referred to in Viaplay Group's Data Protection policy, clarifying that the DPO is appointed formal DPO for all entities within Viaplay Group, and minor editorial changes.
4	2022-01-11	Clarified the role of the Central Data Protection Team and also further developed the role of Head of Privacy (previously "Central DPO"). Changed ownership of document to Head of Privacy.
5	2022-09-12	No changes
6	2023-11-28	Substantial editorial changes and substantial content changes due to internal restructuring. Introduced new roles and responsibilities within Viaplay Group's Privacy Team (local DPOs and Group DPO). Introduced and developed the Data Protection Governance Model, consisting of three layers. Introduced an additional member of the Central Data Protection Team. Introduced RACI approach in the Privacy Programme. Changed ownership of document to Group Data Protection Officer.
7	2024-10-28	Minor editorial and linguistic changes. Clarified the role of Internal Audit. Revised responsibilities of the different teams in the Tasks Framework.
8	2025-12-01	Comprehensive linguistic and structural clarifications to improve readability and consistency; harmonised terminology across roles and layers; clarified descriptions of the governance, control (three lines of defence) and operational layers; removed redundancies and overlaps without changing the underlying governance model, roles or responsibilities.