Data Protection Governance Directive

Document owner	Group Data Protection Officer
Approval	CEO and CFO
Initially adopted	3 September 2018
Date last approved	December 2024
Date of next review/approval	Q4 2024
Applicability	Group

Data Protection Governance Directive

1. Introduction

As we navigate an increasingly digital landscape, the responsible and ethical management of personal data has become paramount. Recognising the pivotal role that data protection plays in our operations, Viaplay Group is committed to establishing a comprehensive framework that ensures the lawful, secure, and transparent processing of personal data.

This Data Protection Governance Directive serves as a cornerstone for guiding our organisation in upholding the highest standards of data protection, adhering to relevant legal requirements, and safeguarding the trust of our stakeholders. By implementing robust governance measures, we aim to foster a culture of accountability, transparency, and respect for individual privacy within the fabric of our operations. This Directive describes how Viaplay Group works with data protection from a governance as well as material perspective.

1.1. Target group

This Group Directive applies to Viaplay Group and to its subsidiaries and controlled entities. The persons specified in the following table are obliged to read this Directive.

Target Group	Motivation
Members of the Group Executive Team and Country Leadership Teams	Accountable for adherence to the principles set out in this Group Directive and for ensuring allocation of appropriate resources and support.
Members of Function Management Teams	Need to know the content of this Group Directive to build a data privacy awareness culture and to ensure allocation of appropriate resources within their respective area.
Group DPO, Local DPOs, and Central Data Protection Team	Need to know the content of this Group Directive and act in accordance with their defined roles and responsibilities.
All employees in Viaplay Group's Legal and Compliance functions	Need to know the content of this Group Directive and to adhere to the principles set out in this Group Directive and other Group data protection policies and guidelines in their legal advice and decision-making.

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 – the EU General Data Protection Regulation (GDPR) and national data protection legislation.

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.

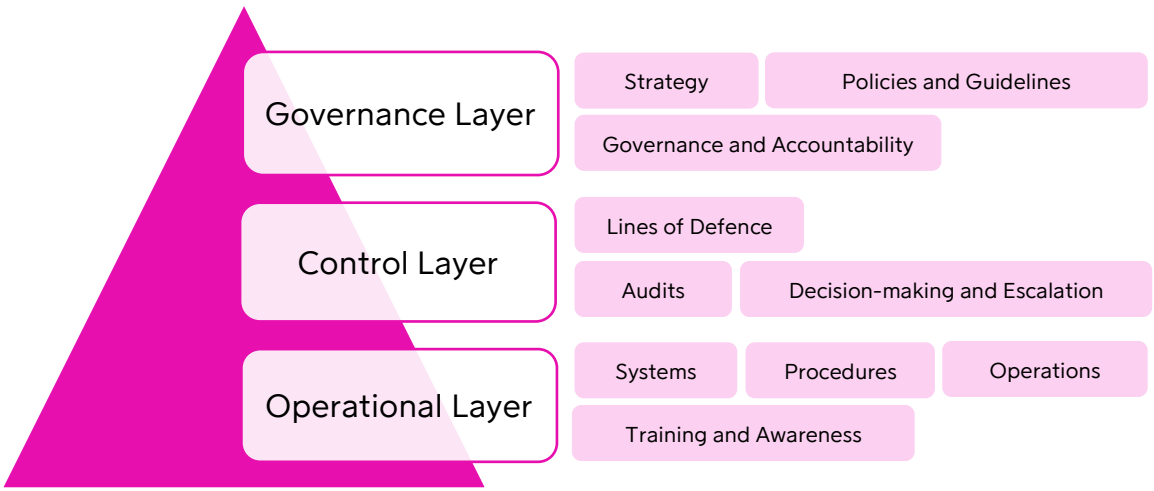
Processor – a natural person or legal entity that processes personal data on behalf of a data controller.

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

The Governance Layer establishes the foundational framework for our data protection initiatives, organising a robust governance structure that meticulously defines roles, responsibilities, policies, and overarching principles. This layer serves as the bedrock, ensuring that our strategical approach aligns seamlessly with regulatory requirements and industry best practices.

2.1.1. Strategy and principles

Viaplay Group should be regarded as a reputable and trustworthy organisation, distinguished for its commitment to upholding standards in the field of data protection. Consequently, adherence to the provisions stipulated in the GDPR and relevant data protection legislation is imperative. The safeguarding and processing of personal data at Viaplay Group is grounded in the principles outlined in **Viaplay Group's Data Protection Group Policy**. Conforming to these principles is essential to guarantee the lawful and secure handling of personal data.

2.1.2. Risks of non-compliance

Unlawful processing of personal data or a breach of personal data may constitute a failure to comply with data protection legislation. Such non-compliance can result in serious consequences for Viaplay Group, including damage to the organisation's reputation, loss of trust from critical stakeholders such as customers, employees, suppliers, and regulatory bodies, and substantial financial penalties for the organisation. Additionally, in some jurisdictions, the consequences may extend to criminal liability.

Non-compliance with the GDPR may result in 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.

2.1.3. Roles and responsibilities

Four key figures bear the highest level of responsibility for ensuring compliance with data protection legislation.

Corporate

Head of Corporate Compliance

- Assessing third-party management on data protection practices
- Responsible for internal corporate distribution of processes
- Coordinating with Group DPO on data protection compliance priorities
- Monitoring regulatory initiatives and advising on actions

Head of Information Technology

- Aligning IT security initiatives with Group data protection policies
- Monitoring data protection settings for Group systems/assets

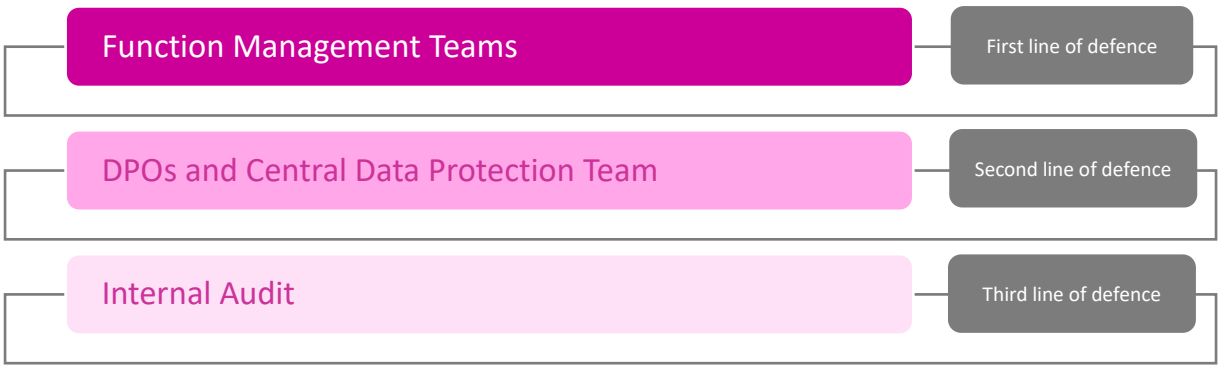
Local	**Local DPOs** • Point of contact with the local Supervisory Authority and data subjects • Cooperation with the Supervisory Authority • Data protection advice to the appointed organisation/market • Control and monitoring of compliance of the company/market • Training and raising awareness on data protection matters • Monitoring of processing activities records (Art.30 GDPR) • Review, evaluate, and assess security breach communication • Monitoring of exercise of data subject rights • Implementation of Group data protection policies and guidelines
Group	**Group Data Protection Officer** • Monitoring the data protection compliance of the Group • Consolidated reporting to the highest management of the Group • Point of communication with the Supervisory Authorities at Group level • Coordinating the work of local DPOs and Central Data Protection Team • Impact assessment of security incidents at Group level • Data protection advice at Group level • Monitoring of implementation of Group data protection policies • Managing data protection related queries at Group level • Perform data protection impact assessments at Group level • Facilitate corporate criteria and be the point of contact at a corporate level for the local DPOs

2.2. Control Layer

Our governance model incorporates a sophisticated control framework based on the three lines of defence. This strategic approach empowers Viaplay Group to proactively identify, assess, and mitigate risks, reinforcing our commitment to the highest standards of data protection. By integrating effective monitoring and control mechanisms, we fortify our defences against potential threats and demonstrate our dedication to the responsible stewardship of personal data.

2.2.1. Lines of Defence

The data protection governance model fits into the Group governance model. Viaplay Group's approach to data protection is based on the principle of three lines of defence, each with specific ownership, control, and assurance responsibilities.



Viaplay Group adopts a risk-based approach towards data protection. Each function is encouraged to prioritise the mitigation of immediate or higher-level risks, maintaining a balanced consideration of risks and corresponding mitigation actions. This approach factors in the specific nature, scope, context, and purposes of the data processing activities within each function. While Viaplay Group's Privacy Team, led by the Group Data Protection Officer and supported by local Data Protection Officers, establishes the overarching framework for our data protection efforts, it is essential to note that ownership of privacy risks is vested within each function. This decentralised ownership ensures that every department is actively engaged in safeguarding data privacy in alignment with the established framework.

2.2.2. First line of defence – function level

Function Management Teams. The Function Management Teams of Viaplay Group are responsible for the implementation of, and adherence to, Group data protection policies and directives. It is incumbent upon them to integrate data protection principles into day-to-day business activities and processes, allocating necessary resources to ensure compliance. Furthermore, the Function Management Teams are tasked with the implementation of Viaplay Group's Data Protection & Security Management System (see Section 2.3.1) within their respective domain. In instances where appointed local Data Protection Officers identify data protection risks, they are empowered to escalate these concerns and request decisions from the Function Management Teams. As a result, the Function Management Teams shall incorporate data protection as a recurring item on their meeting agendas, ensuring its consideration at least on a quarterly basis. This proactive approach underscores the commitment to robust data protection practices within the functional areas of the organisation.

2.2.3. Second line of defence – local and central level

Local Data Protection Officers. Viaplay Group has formally appointed local DPOs for those entities within the Group where any of the following assumptions are met by that entity:

- regular and systematic monitoring of data subjects on a large scale are part of its core activities;
- processing of large scale special categories of data forms part of its core activities;
- where the local laws require the designation of a DPO.

Local DPOs respond directly to the local competent Supervisory Authority and the data subjects and support the Group DPO in fulfilling the requirements of applicable data protection legislation. Local DPOs are the primary contact persons for data protection queries within their appointed organisation/market. They are responsible for advising on, identifying, managing/coordinating, and implementing the following data protection activities:

- raising awareness of data protection issues within their organisation, including maintenance and deployment of training resources (with assistance from Group DPO);
- implementing Group data protection policies and guidelines;
- maintaining a record of processing activities and systems/assets containing personal data within their organisations in OneTrust, including approving new processing activities and systems;
- assisting in managing data subject access requests from customers, business partners and employees;
- supporting the execution of Data Protection Impact Assessments;
- assessing whether legislative changes require adaptation of business processes and coordinating any such adaptation (in consultation with Group DPO);
- coordinating audits of third-party processors (when reasonably deemed necessary and in cooperation with Viaplay Group's IT/Information Security teams);
- assisting stakeholders within their organisation and legal counsels with negotiations of Data Processing Agreements;
- reporting and/or managing personal data breaches within their organisations;
- submitting a Data Privacy Governance Report to Group DPO with a summary of all data protection-related activities, GDPR-specific risks, incidents, breaches and mitigation actions, as well as recommendations for follow-up actions and improvements for their respective organisation;

Group Data Protection Officer. The Group DPO is Viaplay Group's senior advisor on data protection matters. The Group DPO is responsible for maintaining Viaplay Group's data protection framework (preparing and updating policies, templates and other guidance documents related to data protection for the Group) and for advising on and monitoring the Group's compliance with data protection legislation, Viaplay Group's Code of Conduct and Group policies, and for identifying and coordinating mitigating actions when necessary. The Group DPO shall have the following responsibilities:

- establishing, deploying and maintaining data protection training activities for Viaplay Group employees;
- establishing Viaplay Group's annual data protection roadmap, which indicates the main activities on Group level and within the functions for the following year;
- establishing the yearly Governance wheel which sets out the GDPR key stones to be reviewed, updated and maintained throughout the year;
- serving as a contact point for appointed DPOs and giving advice, recommendations and updates on data protection issues and legislation;
- advising in relation to new or amended data processing activities;
- serving as the principal contact point between Viaplay Group and supervisory authorities;
- updating the Central Data Protection Team on relevant developments in the field of data protection;
- compiling summaries of received data protection reports for the Central Data Protection team, including recommendations for follow-up and improvements;

- reporting data protection-related risks and issues to Viaplay Group's Audit Committee and the GRC.

Independence and authority are important for the fulfilment of the DPO role. To exercise the role in compliance with the GDPR, 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 hindrance from management;
- should have direct access to the highest management level;
- is entitled to address issues to Internal Audit and to the Board of Directors of legal entities for further investigations;
- is bound by confidentiality concerning the performance of his/her duties in accordance with the law;
- should not be instructed, dismissed or penalised by a data controller or data processor for exercising his/her duties;
- can document and escalate as necessary in the event of objections to his/her guidance;
- can exercise additional duties, but the organisation should ensure that such duties do not result in a conflict of interests;
- should receive necessary resources to exercise his/her duties and to maintain expert knowledge in data protection.

Central Data Protection Team. This team aims to synchronize the data protection work between Viaplay Group's Privacy Team and Viaplay Group's 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 Corporate Compliance, and Head of IT. Representatives from other business areas and Group functions can be invited when necessary. Meetings should be held when necessary and at least on a quarterly basis. The Central Data Protection Team has the following responsibilities:

- making decisions on data protection issues that impact the Group or several organisations/markets;
- creating a bridge between data protection and IT/Information Security matters and allocating ownership;
- escalating major data protection issues (involving high risks and/or extra investments/costs).

2.2.4. Third line of defence – central level

Internal Audit. Internal Audit should ensure that data protection compliance audits are carried out on a regular basis. Additionally, they should oversee the adherence of Viaplay Group to its data protection program and its compliance with data protection legislation, Group Policies and Directives.

2.3. Operational Layer

At the operational level, our model unfolds a set of finely tuned processes, procedures, and operations, constituting the operational backbone that provides essential support for GDPR compliance. This layer ensure that our day-to-day activities align with the established governance structure and adhere to the prescribed policies, thereby creating a harmonious synergy between our strategic intent and practical execution. Viaplay Group is required to implement appropriate technical and organisational measures to guarantee and demonstrate that the processing of personal data is performed in compliance with the applicable data protection legislation.

To successfully handle the proper management of compliance with data protection regulations, a number of components must work in accordance with the stated strategy and the outlined framework.

2.3.1. Data Protection & Security Management System

Viaplay Group operates a Data Protection & Security Management System that is implemented locally. The system contains information necessary to demonstrate compliance with data protection legislation and related Info & IT Security rules.

As part of this system, Viaplay Group uses OneTrust to map out personal data processing across the organisation. It also helps us identify 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 Data Protection & Security Management System contains the following documentation and information, among others:

- 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 (OneTrust);
- Legitimate Interest Assessments (OneTrust)
- Data Protection Impact Assessments (OneTrust);
- 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 (Jira);
- Records of Data Subject Rights Requests (Jira);
- Annual Data Protection Governance Reports;
- Records of employee data protection training activities.

2.3.2. Relationships between Viaplay Group's legal entities

Functional areas within Viaplay Group do not have any legal rights or obligations under data protection legislation. Such rights and obligations are solely allocated to legal entities.

The legal entities are either to be regarded as data controllers, joint controllers, or processors for each process. If one legal entity within Viaplay Group is regarded as a data controller and the other legal entity as a processor, the entities should enter into a data processing agreement, regardless of whether the legal entities are assigned to the same business area. Viaplay Group has Intra Group Data Processing and Transfer Agreement in place that covers transfer of data between legal entities.

If the entity is a joint controller and has established the purpose and means of data processing together with one or more additional entities, a joint controller arrangement should regulate each entity's responsibility for compliance with 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	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	R	R, A	I		
Complete vendor security assessments	C	C	R, A		
Identify and document data breaches	C, I	I	R, A		I
Assess breach response procedure and notification	R, A	C	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			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.