Group Data Protection Policy

Document owner	Group Data Protection Officer
Approval	Board of Directors
Initially adopted	15 June 2018
Date last approved	19 September 2024
Date of next review/approval	Q3 2025
Applicability	Group

Group Data Protection Policy

1. Introduction

1.1 Aim of this Policy

Viaplay Group AB (publ.) ('**Viaplay Group**' or the '**Company**') considers the safeguarding of data protection and privacy rights as part of its social responsibility.

Viaplay Group places significant importance on the protection and appropriate processing of personal data, including the personal data of its employees, contractors, customers, partners, stakeholders and other parties. All concerned parties shall be made aware of the importance of handling and protecting personal data in a fair and transparent way and in compliance with the applicable laws and regulations.

This Group Data Protection Policy ('**Policy**') establishes uniform and suitable data protection standards and guidance for processing personal data in accordance with applicable laws, such as the EU's General Data Protection Regulation 2016/679 ('**GDPR**'), within Viaplay Group, regardless of whether the processing of personal data occurs within or outside the EU/EEA region.

1.2 Scope and applicability

This Policy applies to Viaplay Group, its controlled group companies and subsidiaries, and all employees in which Viaplay Group exercises decisive control (directly or indirectly), including consultants and freelancers contracted to perform services for Viaplay Group.

This Policy applies to fully or partially automated processing of personal data, as well as manual processing in filing systems unless national laws provide for a broader scope. The Policy also applies for the development of tools, products and services used to process personal data by Viaplay Group.

This Policy does not replace EU legislation and national laws on privacy and data protection. It is meant to supplement them. Where the applicable legislation requires a higher level of protection for personal data, it will take precedence over the Policy. In the absence of corresponding national laws, this Policy applies.

In the event of conflicts between national laws and this Policy, the Group Data Protection Officer and the central compliance organisation will work to find a practical solution that fulfils the purpose of this Policy.

1.3 Legal enforceability

The rules and provisions of this Policy are binding to Viaplay Group operating within its scope of application. Noncompliance with this Policy may result with serious consequences for both Viaplay Group and the individuals concerned. Viaplay Group faces substantial fines as well as damage to its reputation and shareholder value in such cases.

Individual employees may face personal penalties and disciplinary action, as well as termination of employment and criminal sanctions. In addition to the applicable EU legislation and national data protection laws, Viaplay Group, as well as its management and employees, are responsible for compliance with this Policy.

This Policy does not address every situation that may occur when processing personal data. For any concerns or questions relating to data protection matters, stakeholders shall contact the Group Data Protection Officer or their locally appointed Data Protection Officer.

2. Responsibility and Implementation

2.1 Responsibility

This Policy is owned by the Group Data Protection Officer, who together with the locally designated Data Protection Officers, is responsible for maintaining and updating the Policy, as well as for ensuring that it is appropriately published and enforced.

The members of the Group Executive Management Team and all members of managing bodies of the Company are responsible for communicating and implementing this Group Policy, and for ensuring that all employees within their area of responsibility are familiar with and follow this Policy. Therefore, they are required to ensure that the legal requirements for data protection, and those contained in this Policy, are met.

All Viaplay Group employees, consultants, and freelancers are individually responsible for reading, understanding, and adhering to this Policy when applicable. Employees are urged to raise concerns about any actual or potential violations of this Policy to their line manager, local Data Protection Officer, Group Data Protection Officer, or via the whistleblower channels.

2.2 Awareness raising and training.

If employees have constant or regular access to personal data, participate in data collection or the creation of tools used to process personal data, or are involved in any of these activities, management is responsible for ensuring that employees receive and attend the necessary data protection training, including the content and handling of this Policy.

All employees shall complete a general training on privacy and data protection at least once in a calendar year.

2.3 Organisation

The group-wide data privacy organisation at Viaplay Group is coordinated by the Group Data Protection Officer, who, together with the locally appointed Data Protection Officers, comprise the Privacy Team.

The Group Data Protection Officer is internally independent of instructions regarding

the performance of his/her tasks. Each individual is responsible for this Policy, monitors its implementation and must ensure compliance with national and international data protection laws. The Group Data Protection Officer reports directly to the Board of Directors of Viaplay Group AB (publ.) and of all companies for which he/she has been appointed. The Board of Directors shall be informed of the annual report of the Group Data Protection Officer as part of existing reporting duties.

Companies within Viaplay Group may appoint their own Data Protection Officer with prior consultation with the Group Data Protection Officer. All Data Protection Officers shall be jointly responsible for compliance with national and international data protection laws. Locally appointed Data Protection Officers report to the highest management level of their designated company and cannot receive any instructions for the performance of their tasks.

2.4 Audit and controls.

Compliance with this Policy and applicable data protection laws shall be reviewed at Group level on a regular basis, at least once in a calendar year, on a risk-based approach, or on a specific request from the Group Data Protection Officer, through an internal compliance risk assessment, audits including on specific data protection topics and other checks. The results shall be reported to the Group Data Protection Officer, the responsible company and its Data Protection Officer, if one has been appointed.

2.5 Risk assessments and governance.

The Privacy Team publishes its Governance Wheel outlining the privacy focus areas to be prioritized on an annual basis. The wheel is published on Viaplay Group's intranet pages and ensures that the main GDPR pillars are regularly followed up on, re-evaluated, assessed, and maintained. Viaplay Group commits to performing regular risk assessments of its privacy practices and systems across the organization, as well as mitigating any risks associated with them.

Viaplay Group documents, audits, and assesses all processing activities, suppliers, vendors, and systems through its privacy management tool. Employees, consultants, and freelancers commit to supporting this work and reporting to the Privacy Team anything that may have an influence on the privacy practices and the way personal data are processed by Viaplay Group.

3. General Data Protection Principles

3.1 Scope of protection

This Policy applies to any processing of personal data by Viaplay Group. '**Personal data**' is any information that could, directly or indirectly, identify a living person. Examples include name, social security number, email address or physical address of a living person, if the information (stand alone or in combination with other information) is sufficient to identify the person. Employee or customer numbers, unique identifiers, online identifiers, IP

addresses, location data, behavioural data, genetic data, and other information that can be backtracked or indirectly linked to a living person are other examples of personal data. Certain types of cookies may also involve the processing of personal data.

Completely anonymized information, i.e., information that cannot be used to identify a living person in any way, does not constitute personal data. However, pseudonymized or encrypted information still constitutes personal data if it is possible to unlock the information. In general, it makes no difference who owns the key to unlocking such information.

Any handling of personal data constitutes '**processing**', and thus falls under the provisions of the GDPR and this Policy. This includes collecting, using, storing, structuring, transferring, or deleting personal data.

Viaplay Group is committed to processing personal data in compliance with its responsibilities under the GDPR and other data protection legislation as applicable. The Company is committed to incorporating leading data protection standards into all processing activities and systems, as well as establishing adequate technical and organizational security measures to protect personal data against unauthorized access, unwanted changes, and data loss.

3.2 Lawfulness, fairness, and transparency

Personal data must be processed in a lawful manner and in good faith. Each processing must be based on one of the legal grounds established by the GDPR and shall be carried out in a way that an individual would reasonably expect. The legal basis must be established before any processing can begin. The following legal bases are most applicable to Viaplay Group:

i) The individual has freely given, specific, informed, and unambiguous **consent** to the processing. Consent must be expressed by a statement or clear affirmative action from the individual, such as ticking a box on a website, choosing technical settings for information society services, or another statement or action that clearly indicates consent to the processing. Silence, pre-ticked boxes, or inactivity should never be utilised to obtain consent. In addition, there must be a simple way for the individual to withdraw his/her consent, i.e., withdrawing consent must be as easy as giving it.

ii) Viaplay Group must process the personal data to **fulfil a contract** with the individual, for example performing ordered services, billing, or delivering ordered products or services, or performing obligations under an employment contract.

iii) Viaplay Group has a **legitimate interest** in processing the personal data, which means that Viaplay Group's interest in processing the data in the given situation is deemed to outweigh the interests and rights of the individual.

iv) Viaplay Group needs to process the personal data to comply with a **legal obligation.**

The legal basis for processing personal data must be clear, documented and communicated to the individual. As a result, privacy policies and notices must always be present on websites and other platforms, and they shall be referred to while collecting personal data. The responsible process owner must inform the data subjects of the purposes and circumstances of the processing of their personal data. This information must be given in a concise, transparent, intelligible, and easily accessible form whenever the personal data is collected for the first time.

3.3 Purpose limitation

Personal data may only be processed for the legitimate purpose specified before collecting the data. Subsequent changes to the purpose of processing are only permitted if the processing is compatible with the initial purpose for which the personal data was collected.

3.4 Data minimisation

Personal data shall be collected only to the extent strictly necessary for the fulfilment of the defined purposes. Personal data shall not be collected because it may be useful in the future. Where the circumstances and purposes allow, anonymised or pseudonymised data must be used.

3.5 Data accuracy

Personal data stored must be objectively accurate, and if applicable, up to date. Reasonable steps should be taken to ensure that inaccurate data are corrected, updated, or deleted without delay.

3.6 Retention (storage limitation)

Personal data may only be stored for as long as necessary to achieve the specified purpose, after which the data must be destroyed or anonymised. Individual process owners shall ensure that they implement time limits for retention and either erase or anonymise data when that period has passed, and the purposes have been fulfilled. Each system used at or by Viaplay Group must have a deletion routine, either manual or automated.

3.7 Security (integrity and confidentiality)

Personal data shall be processed in a way that ensures the data stays secure. This includes using appropriate technical and/or organisational measures to protect the personal data against accidental, unauthorised or unlawful access, modification, disclosure, loss, destruction and/or damage.

Those processing personal data are obliged to safeguard the integrity and confidentiality of the data by implementing measures such as pseudonymisation and encryption. When new methods of data processing (e.g., new IT systems are introduced), appropriate technical and organisational measures shall be implemented, taking into account the

state of the art, the cost of implementation, as well as the risk and severity for the rights and freedoms of the data subjects.

3.8 Accountability

Viaplay Group is obliged to ensure compliance with applicable data protection laws and regulations, as well as demonstrate such compliance.

Before initiating any personal data processing, process owners must document the procedures in which personal data in a Record of Processing Activities. This record shall be maintained in writing in electronic form and should be made available to the relevant supervisory authority upon request. Requirements established by the Privacy Team on documentation (such as software tools and documentation instructions) must be observed.

4. Specific considerations

4.1 Rights of data subjects

An individual whose data are processed by Viaplay Group has the following rights:

- the right to be informed of the processing of their personal data;
- the right to obtain information about how their data is processed, and receive a copy of their personal data (unless interests of third parties worthy of protection prohibit this);
- the right to correct or supplement personal data if they are incorrect or incomplete;
- the right to delete their personal data, under certain circumstances;
- the right to temporarily restrict the processing of their data if they dispute the accuracy, the processing is unlawful, the data is not necessary for the processing purpose but must be kept for legal claims, or a decision is pending upon objection on the legitimate interests of Viaplay Group for the processing;
- the right to receive their personal data which are provided on the basis of consent, or in the context of an agreement that was concluded with the data subject, in a commonly used digital format;
- the right to object to direct marketing, or to any processing based on the legal basis of overriding legitimate interests of Viaplay Group, or to any processing by automated means in the context of information society services.

Individuals are entitled to exercise any of the above rights by contacting Viaplay Group via designated channels. Such inquiries must be answered within one month of receipt of the request. Considering the complexity and number of requests, that one month period may be extended at maximum by two further months, in which case the individual must be informed accordingly of the reasons for the delay.

4.2 Transfer of personal data within Viaplay Group

Transferring personal data to other companies within Viaplay Group must be evaluated on a case-by-case basis, and the legal basis for such transfer must be established. The specific circumstances of the transfer (particularly data categories, means of transfer, and further transfer to a third party) must be considered, as must the laws and practices applicable to the Group Company in the third country, including those requiring data disclosure to public authorities or authorizing access by such authorities.

Viaplay Group and its subsidiaries and affiliates have entered into an Intra-Group Data Agreement which regulates the respective responsibilities and obligations for personal data transfers between the companies.

Transfer of personal data outside the EEA

As a main rule, personal data may only be processed within the European Economic Area (EAA). Viaplay Group may only transfer personal data from the EEA to third parties outside the EEA, if any of the following safeguards are in place:

i) data is transferred to a third country that provides an adequate level of protection recognised by the European Commission;
ii) the transfer is subject to EU standard contractual clauses signed by Viaplay Group and the third party receiving the data (with supplementary measures to ensure an essentially equivalent level of protection as provided in the EEA, if needed);
iii) there are Binding Corporate Rules in place with the third party to which the data is transferred (with supplementary measures to ensure an essentially equivalent level of protection as provided in the EEA, if needed).

Viaplay Group undertakes to store personal data within the EEA to the furthest extent possible. If third parties are used to process personal data on Viaplay Group's behalf (for example, to store personal data, create marketing campaigns, provide services to customers, etc.), the Company must enter into a written data processing agreement or a data sharing agreement with such supplier. The choice of the agreement will depend on the respective roles and responsibilities of the parties. These agreements aim to ensure that such party complies with applicable data protection laws and acts in accordance with this Policy or other standards consistent with the level of protection established by this Policy. All data processing agreements must be signed and uploaded in the Company's contract management platform. Third parties may also be subject to audits performed by Viaplay Group, whether on site or otherwise, to ensure such parties can safeguard and adequately protect Viaplay Group's personal data.

4.3 Working With Third Parties

When engaging or retaining a new third-party that can view, collect, process, and/or access the personal data of Viaplay Group's customers or employees, Viaplay Group shall conduct a third-party due diligence through its Business Integrity Screening (BIS) process. A BIS helps us keep accurate records, adhere to laws and regulations, and

ultimately ensures that all requirements under this policy are met when you engage with third parties. For this purpose, third party is any company or individual not belonging to Viaplay Group, including all suppliers, service providers, resellers, distributors, consultants, sales channel partners, subcontractors, and other business partners. To help you understand the BIS process, refer to the BIS Guidelines on Viaplay Group's Group Compliance intranet page.

4.4 Data Protection Impact Assessment

When introducing new data processing, or in the event of a significant change to an existing processing (especially through the use of new technologies), Viaplay Group is obliged to assess whether this processing poses a high risk to the privacy of data subjects. As a first stage, an initial risk assessment shall be done to assess whether a DPIA is required. When the risk assessment suggests a high risk for the data subjects, the responsible process owner carries out a so-called Data Protection Impact Assessment (DPIA) with the aim to identify and attend all possible processing risks at an early stage. A DPIA is required when new technologies are used or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

Examples of processing likely to result in a high risk include:

- systematic and extensive processing activities, including profiling where decisions have legal or similarly significant effects on individuals;
- large-scale processing of special categories of data or personal data relating to criminal convictions or offences;
- large-scale, systematic monitoring of public areas (CCTV).

The Privacy Team shall assist the process owners in carrying out the DPIA and advise on appropriate measures for risk reduction if the assessment results show a high risk to the rights and freedoms of individuals.

4.5 Data protection by design and by default

To safeguard privacy-related interests throughout the entire life cycle of its processing activities, Viaplay Group shall implement technical and organisational measures to ensure the data protection principles are effectively implemented. Viaplay Group shall define state-of-the-art strategies and adopt measures to integrate data protection principles into the specifications and architecture of business processes and IT systems for data processing from the beginning, ensuring the most integrity-friendly setting is offered as a default in its services.

4.6 Data breach notification

Viaplay Group has an obligation to protect the personal data it processes. In the event of a data breach, the Company has investigation, information and damage mitigation obligations. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. Viaplay Group must ensure that any data breach is mitigated and, where possible,

the personal data returned to Viaplay Group. Where the personal data breach is likely to result in a risk to the rights and freedoms of individuals, Viaplay Group must, without undue delay and, where feasible, within 72 hours of becoming aware of the breach, inform the supervisory authority of the corresponding breach.

All personal data breaches should be reported immediately after discovery via the Service desk. Any personal data breach should be documented, and the documentation should be made available to the supervisory authority on request.

5. Document History and Change Information

More details about this document's history and change are contained in Appendix 1.

Appendix 1 - Document History and Change Information

Version	Revision Date	Change information
1	2018-06-15	Initial Group Policy
2	2019-09-23	Editorial changes and updated description on how to report a Data Breach.
2.1	2019-10-23	Changes in roles and responsibilities due to internal reorganisation. New Document owner and Local CEOs replaced by Members of the Group Executive Management team and the Extended Management team.
3	2020-09-24	Editorial changes and updates in the text about where to store data processing agreements (p. 4.2), transfers outside the EEA (p. 4.3) and performance of DPIA (p. 4.4).
4	2021-09-21	Editorial changes and updates in the text about transfers outside the EEA (p. 4.3). Added consultants and freelancers to target group, and consequences of possible breach of this policy (p. 2). Added a section on Compliance with Group Policy (p. 3), risks assessments and Governance wheel (p. 5.7). Changes in roles and responsibilities due to internal reorganisation and change in ownership of Group Policy (p. 6).
5	2022-09-22	Editorial changes and updated description on how to report a Data breach as it will now be performed through service desk. Added information in section 5.2 regarding intragroup transfers.
6	2023-09-21	Substantial editorial changes and updated sections on responsibility and implementation, introducing a new group-wide data privacy organisation and roles due to internal reorganisaiton. New Document Owner due to internal reorganisation.
7	2024-08-26	Editorial changes and introduction of an obligation to perform due diligence when engaging with third parties (p.7).