Group Whistleblower Directive

Document owner	Head of Group Compliance
Approval	CEO/CFO
Initially adopted	10 October 2018
Date last approved	22 December 2025
Date of next review/approval	Q4 2026
Applicability	Group

Group Whistleblower Directive

1. Introduction

Viaplay Group AB ('**Viaplay Group**') conducts business with responsibility, honesty, and integrity expects the same from everyone who works with or for us. We strive to promote a culture of openness and accountability.

The purpose of this Directive is to enable and encourage individuals to report suspected or observed incidents of serious misconduct. We want everyone at Viaplay Group to know that concerns will be taken seriously and handled appropriately, reports will be investigated in a fair and timely way, confidentiality will be respected, and no one will be subject to retaliation for reporting in good faith.

2. Target Group

This Directive applies to all individuals who, in a work-related context, work for or with Viaplay Group and its subsidiaries and entities in which Viaplay Group exercises decisive control (directly or indirectly), including ('**Workers**'):

- senior executives, managers, directors, and employees (permanent, fixed-term, or temporary),
- job applicants, consultants, contractors, interns and trainees,
- employees of partners and suppliers with whom Viaplay Group has an established work-related relationship,
- persons whose work-related relationship with Viaplay Group has ended, if the information was received or obtained during that relationship,
- other persons who in a work-related context perform work for, on behalf of, Viaplay Group.

Use of the whistleblowing channel under this Directive is voluntary.

3. Principles and Procedures

3.1. What should I report in the whistleblowing service?

The whistleblowing service is for reporting witnessed or suspected misconduct in a work-related context that has occurred, is very likely to occur, is ongoing, and where there is a **public interest** in the disclosure.

Misconduct in the public interest

Misconduct that warrants disclosure in the interest of the public generally involves actions or omissions that:

- violate regulations or laws, or
- violate directly applicable EU law or national rules implementing or supplementing such laws (as defined in the EU Whistleblowing Directive[1]).[2]

[1] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law.
2 For a complete list of relevant Union law acts, see: https://eur-lex.europa.eu/legal-

Examples of areas covered include, among others:

- public procurement,
- financial services, products and markets,
- prevention of money laundering and terrorist financing,
- environmental protection,
- public health,
- consumer protection,
- privacy and personal data protection, and
- security of network and information systems.

In line with the above, certain acts or omissions contrary to **Viaplay Group 's Code of Conduct** or **Third Party Code of Conduct** also fall within the scope of this Directive, such as anti-corruption, competition, sanctions compliance, intellectual property, data protection, and information security matters.

Own employment matters

Information relating **only** to your own working or employment conditions will normally not be considered of a public interest and is therefore **not** typically a whistleblowing matter. Exceptions include, for example:

- labour exploitation of minors or working conditions resembling slavery, or
- an employer's systematic violations of applicable regulations towards an employee.

Section 3.2 below explains what should not normally be reported through the whistleblowing service. If you are unsure whether your concern qualifies as a whistleblowing matter, you may seek guidance from Viaplay Group's Whistleblower Officers.

Good faith and misuse of the system

Anyone submitting a report must act honestly and in good faith. Reports must not be made with malicious intent or with knowledge that the allegation is false. Viaplay Group takes any abuse of the whistleblowing system seriously and such conduct may lead to disciplinary action.

3.2. What should I not report in the whistleblowing service?

The whistleblowing system is **not** intended for:

- work environment concerns (e.g., workload, ergonomics, safety issues that are not serious legal breaches),
- minor misconduct,
- dissatisfaction with management style,
- difficulties in cooperating with people,
- general workplace dissatisfaction,
- inefficient systems, or
- other operational feedback or issues related to standard HR processes or employment terms and conditions.

Such issues should be raised through usual reporting lines outlined in Viaplay Group's Work Environment Policy, either by contacting your line manager, manager's manager, or your local People & Culture Business Partner. Openness and direct dialogue generally make it easier for

content/SV/TXT/PDF/?uri=CELEX:32019L1937&from=en#page=31.

Viaplay Group to assess and investigate the matter.

Exception – serious personal misconduct

Cases involving **gross personal misconduct that may constitute a crime**, such as modern slavery, human trafficking, child labour, or other similarly serious offences, **should** be reported via the whistleblowing channels.

3.3. How to report?

If you observe conduct that you believe falls within the scope of this Directive (see Sections 3.1 and 3.2), you are encouraged to report it through one of the following internal channels:

- **Option 1: Group-level reporting via Viaplay Group's Speak-Up Line :** You may submit a written report, an oral report, or a request for a virtual or in-person meeting through Viaplay Group's joint whistleblowing channel – the Speak-Up Line. Reports made via the Speak-Up Line are forwarded to one of the Group's Whistleblower Officers to facilitate additional communication and inquiry.

  More information on how the Speak-Up Line operates is available in **Appendix 1 – Internal Reporting and Data Protection**, Section 3.

- **Option 2: Local whistleblowing channel (currently, only available for reporting violations concerning operations of Viaplay Group Sweden AB).** You may submit a written report, an oral report, or a request for a virtual or in-person meeting with your local subsidiary within Viaplay Group using locally available whistleblowing channels. Your report will be passed to one of Viaplay Group 's Local Whistleblower Officers for further communication and inquiry.

  For comprehensive information regarding local deviations from this Directive, see **Appendix 2 (Sweden)** or **Appendix 3 (Denmark).**

Regardless of whether you choose to report through Viaplay Group's joint whistleblowing channel or your local whistleblowing channel, you can choose to make an anonymous report. If so, you will remain anonymous throughout the whole process unless you decide to reveal your identity.

You can access both the Viaplay Group joint whistleblowing channel and your local whistleblowing channel via the following link.

4. External Reporting and Local Rules

4.1. Reporting to an authority

In addition to internal reporting, you may report concerns falls within the scope of this Directive (see Section 3.1) externally to a **competent authority** in an EU country. Authorities maintain reporting channels that are independent from their other activities.

For information about local deviations, please refer to **Appendix 2 (Sweden)** or **Appendix 3 (Denmark).**

If you report externally to a competent authority without using the authority's designated external reporting channel, additional conditions apply. You must either:

- have reported internally, and the recipient failed to take appropriate action or provide feedback within three months from the report; or
- have reasonable grounds to believe that the misconduct involves an imminent or obvious

danger to life, health, safety, or a risk of extensive damage to the environment, or for any other valid reason to report to the authority; or

— have reasonable grounds to believe that internal reporting would entail a risk of retaliation or that the misconduct would not be remedied effectively.

When you report externally, the authority is responsible for receiving the report, following up and providing feedback. Feedback can only be provided if the authority has received sufficient contact information to enable this. The authority is subject to confidentiality in respect of information provided by the reporting person, which can identify the reporting person directly or indirectly. Depending on the nature of the report, the authority may forward the report to competent institutions, bodies, or agencies within the EU.

Depending on the area of reporting, different authorities are responsible for providing a reporting channel. More information on how to report is available on the respective competent authority's website.

4.2. Reporting to EU institutions, bodies, or agencies

If the subject-matter of the report concerns the competence of an EU institution, body, or agency, you may report directly to that institution, body, or agency through its external reporting channels.

4.3. Local rules and precedence

Local laws and regulations in the countries where Viaplay Group conducts its business may supplement or deviate from this Directive. In such a case, the deviant local laws and regulations, provisions, or ordinances shall apply instead of what is stated in this Directive, as appropriate.

For more information on local variations, see **Appendix 2 (Sweden**) or **Appendix 3 (Denmark)**.

5. Confidentiality and Non-Retaliation

5.1. Confidentiality

Viaplay Group will take all reasonable steps to ensure confidentiality throughout the reporting and investigation process. Workers filing anonymous reports should not fear that their identity will be improperly disclosed or abused.

Whistleblower Officers are bound by confidentiality obligations. In an investigation, the whistleblower officers may include persons who add information and/or expertise to the investigation, and in such cases, those persons are also required to observe confidentiality. Informational that may reveal the identity of individuals involved in a case may not be disclosed without proper authorisation.

Viaplay Group will not disclose your identity outside the investigation team, except where:

- disclosure is required by law or regulation,
- disclosure is necessary for follow-up measures within Viaplay Group, or
- information is duly shared with other Viaplay Group entities to implement corrective actions.

Personal data provided via an internal whistleblowing report will be processed in accordance with the principles outlined in **Appendix 1 - Internal Reporting and Data Protection**.

5.2. Non-retaliation

Viaplay Group strictly forbids any form of retaliation or sanction (including harassment, victimisation, or disciplinary action) against any person who reports a concern **in good faith**. Concerns raised in good faith will not expose you to any sanctions, even if the information later proves to be inaccurate or does not lead to further action. Protection against retaliation by the employer is also regulated by law.

Any attempt to victimise, discriminate against or intimidate a person who raises a concern, or who indicates an intention to do so, will not be tolerated and may result in disciplinary action, up to and including dismissal. If a reporter feels they have been retailed in connection to a report, they should file this retaliation case separately in the whistleblowing channel.

Making deliberately false, unfounded or malicious allegations may result in disciplinary action, up to and including dismissal.

You can read more about whistleblowing and your rights and legal protection as a whistleblower on ViaPLACE under Business Ethics.

6. The Process – Internal Reporting

Step 1: Assessment (You)

Before reporting, you should assess whether your concern falls within the scope of this Directive (see Sections 3.1 and 3.2). If you are unsure, you can always ask a Whistleblower Officer.

Step 2: Preparation (You)

You may report anonymously or under your own name.

You are encouraged, where possible, to collect relevant information and supporting material, such as:

- dates and times,
- description of the suspected breach,
- names of persons involved,
- possible witnesses, and
- documents, emails or other evidence.

However, this is **not a requirement**. We do not require a particular level of proof, but you must reasonably believe that the information you provide is substantially true.

Please be aware that your report may lead to decisions that affect other individuals. You should therefore provide information that is accurate to the best of your knowledge, and limit your report information that is adequate, relevant, and necessary for handling and investigating your concerns.

Avoid including irrelevant sensitive personal data, such as non-relevant information about health status, political or religious affiliation, or sexual orientation.

Step 3: Receipt of report (Viaplay Group)

Once a report is received, Whistleblower Officers assess whether it falls under the scope of this Directive. If it does, appropriate investigative steps are taken. If it does not, the Whistleblower Officer may refuse to receive or process the report and will, where possible, inform you of this decision.

A report may be refused if, for example:

- it does not fall within the scope of the whistleblowing service,
- it was not made in good faith,
- there is insufficient information to investigate, or
- the matter has already been handled.

Reports of a primarily HR nature will normally be referred to local HR for further handling.

If an oral report is documented through a transcript or minutes from a meeting, you will be given the opportunity to review, correct, and approve by signing.

Step 4: Investigation (Viaplay Group)

If a report falls under this Directive, Whistleblower Officers will decide whether there is sufficient information to initiate an in-depth investigation. If not, they may contact you for further information, depending on whether you provided contact details.

Investigations will be conducted in a fair, impartial and confidential manner. Reports may not be investigated by anyone who is directly involved in, or affected by, the allegations.

If an investigation is initiated, a Whistleblower Officer will inform you, where possible. This may include:

- invitations to interviews,
- requests for further information, and
- information regarding any broader investigation involving other parties, including the person against allegations have been made.

If you choose to report anonymously, all follow-up questions and requests for additional information will be communicated through the Speak-Up Line.

Step 5: Communication (Viaplay Group)

You will receive:

- confirmation of receipt of your report **within seven days**, and
- feedback **within three months** from the confirmation of receipt, to a reasonable extent, on measures taken or planned as follow-up, and reasons for such measures.

In cases where the investigation has not been completed within three months of receiving the report, you will be informed that additional time is needed for the investigation.

If a decision is made to close the investigation, the decision and the underlying reasons will be communicated to you, where possible.

For anonymous reports, all feedback will be provided through the Speak-Up Line or the communication channel used when the report was submitted.

Step 6: Action (Viaplay Group)

If the concern is found to be valid, Viaplay Group may take one or more of the following actions (non-exhaustive list):

- corrective or remedial measures to address the concern raised,
- referral of the matter to the Chairman of Viaplay Group 's Audit Committee,
- referral of the matter to Viaplay Group's Board of Directors,
- referral of the matter to the relevant external regulatory body, and/or
- referral of the matter to the police.

Viaplay Group may also follow up with the reporter some months after the case has been closed to ensure that no retaliation has occurred. If a reporter believes they have been retaliated against, they should submit a separate retaliation report via the whistleblowing channel.

7. Roles and Responsibilities

The Head of Group Compliance is the document owner of this Whistleblower Directive and responsible for its content.

The document owner is responsible for maintaining and updating the Directive, ensuring that it is properly published, and that it is communicated to and implemented by affected Workers.

8. Further Information

For further information on the processing of personal data in connection with whistleblowing, see **Appendix 1.**

For more information on whistleblowing, visit the **Business Ethics** pages on ViaPLACE.

Any questions or requests for further information regarding this Whistleblower Directive or related procedures should be raised with Head of Group Compliance at compliance@viaplaygroup.com.

9. References

- Appendix 1 – Internal reporting and data protection
- Appendix 2 – Sweden
- Appendix 3 – Denmark
- Appendix 4 – Document history and change information

Appendix 1 - Internal Reporting and Data Protection

1. Privacy Notice

Viaplay Group is committed to respecting the privacy and personal data of everyone at our company. However, in order to investigate concerns from or regarding our people, it may be necessary to process and transfer personal data within Viaplay Group. In such cases, Viaplay Group complies with all applicable data protection rules. In the event of an investigation, we will seek to ensure that we respect individuals' right to privacy as far as possible, and we will process and transfer personal data only when strictly necessary.

2. Data Controller and DPO

All information reported will be evaluated by Viaplay Group and, if necessary, by assigned personnel at our subsidiaries, for the purposes stated in the Internal Reporting/Whistleblowing Group Directive. In such cases, the identity of the Data Controller will be:

Viaplay Group AB
Box 17104
104 62 Stockholm
Sweden
Registration no: 559124-6847

Contact information to Viaplay Group 's Data Protection Officer (DPO):
dpo@viaplaygroup.com

3. Speak-Up Line and Confidentiality

Speak-Up Line is Viaplay Group's Whistleblower tool and it enables individuals to report serious concerns anonymously. The service is operated by a third party, NAVEX Global UK Limited, registered in the United Kingdom with company registration number 12011655 ("Navex"). Navex is responsible for processing all messages received via Speak-Up Line and for transferring them to Viaplay Group in accordance with Viaplay Group's instructions. This means that Navex is, for these purposes, Viaplay Group's Data Processor of personal data. The data is stored on secure servers located in the United Kingdom.

When an individual calls Speak-Up Line via phone, Navex transcribes the message left and then erases the voice recording. Viaplay Group's representatives are unable to hear the individual's voice and Navex will not attempt to trace the individual's caller ID. Similarly, if a message is sent via the Speak-Up website, email addresses are not captured and no attempt is made to identify a user. This means that unless an individual chooses to identify him/herself, there is no way for anyone at Viaplay Group to determine this individual's identity. For more information about Speak-Up Line, see the document "FAQs Speak-Up Line" available on Viaplay Group 's intranet.

4. Processing Personal Data

The processing of personal data is carried out for the purposes of investigating concerns raised by a person filing an internal/whistleblower report (the "Whistleblower"). The personal data will be processed on the legal basis of compliance with a legal obligation to which Viaplay Group is subject or its legitimate interest, as applicable. Viaplay Group's legitimate

interest is to investigate concerns relating to whistleblowing incidents. Any country specific rules regarding the legal basis for the processing of personal data are set out in Appendices 2 – [X].

The personal data processed will usually include personal data held by Viaplay Group regarding the individuals involved, along with any additional data provided by the Whistleblower or data that comes to light during the investigation. Viaplay Group will keep all materials and supporting documentation related to the report in a secure space with restricted access.

Viaplay Group is committed to collecting and processing only personal data that is adequate, relevant and necessary to handle and investigate the concerns raised. Viaplay Group may review the data received, both at the outset of the investigation and on a continuous basis, in order to ensure that only relevant information is retained. Viaplay Group and its assigned personnel handling the investigation will treat all information received in strict confidence. The number of assigned personnel is limited and, as far as possible, Viaplay Group will seek to minimise the transfer of personal data on a strictly need to know basis.

When a Whistleblower's report is received, the assigned Whistleblower Officer(s) determines whether an in-depth investigation is required. Depending on the content of the report, the Viaplay Group personnel responsible for further investigation, normally the Viaplay Group Head of Internal Audit or Group Risk & Security, will receive the information provided by the Whistleblower. The information may also be given to relevant Viaplay Group managers in order to correct shortcomings identified during investigation of the report. If the content of the report is HR related, the relevant HR department will receive the information. Viaplay Group may also involve external specialists such as attorneys, auditors or forensic experts to examine the report as commissioned by Viaplay Group. Finally, if the concerns raised are likely to result in severe consequences for the company, e.g. substantial financial loss, the Viaplay Group Crisis Management team may be involved in the investigation.

Viaplay Group may be required by law to provide courts or government agencies with information relating to compliance violations. In such cases, we are unable to withhold information provided by a Whistleblower.

5. Transferring Personal Data

Personal data provided as part of a whistleblowing report may be transferred to other EEA countries or countries outside the EEA for the purposes of the Whistleblower Directive.

However, personal data is only transferred to countries that offer an adequate level of data protection or where adequate safeguards are in place to ensure protection of the information, such as mechanisms/certifications approved by the EU Commission, standard contractual clauses or binding corporate rules with the third party to which the data is transferred. Please contact dpo@viaplaygroup.com if you have any additional questions relating to transfer of personal data.

6. Notification to Affected Parties

The person identified in a report shall be informed of the processing of personal data that takes place or may take place in connection with the submission of a Whistleblowing Report. This means that the person identified in a report has the right to know what personal data is being processed, from where this data has been collected, the purposes of the processing and to which recipients or categories of recipients the data is disclosed. However, the information must not indicate the identity of the reporting person. This obligation applies provided that this does not lead to obstacles to the investigation or destruction of evidence.

However, information on the processing of personal data shall be provided no later than when action against the accused person is taken.

7. Storing Personal Data

Personal data will be retained for as long as necessary for completion of the investigation, including remediation of any shortcomings discovered and handling of any subsequent legal processes. Personal data will be retained for a longer period if required due to legal, regulatory or contractual obligations, however not longer than 2 years from the completion of the investigation.

Reports to Speak-Up Line are always destroyed 2 months after the investigation is closed.

8. Accessing, Correcting and Deleting Data

Individuals whose personal data is processed are afforded certain rights to access, correct, block and delete such data. However, in a Whistleblower/Internal Reporting context such rights may be restricted, and requests based on these rights will therefore be assessed on a case- by-case basis.

9. Questions and complaints

If you have any questions or concerns about the processing of personal data, you are welcome to contact Viaplay Group 's DPO (dpo@viaplaygroup.com). You may also contact the local Data Protection Authority.

For additional information about how Viaplay Group processes personal data please read Viaplay Group’s Data Protection Policy.

Appendix 2 - Sweden

Scope of applicability

This Appendix applies to whistleblowing taking place in Sweden.

Applicable local law

Sw: Lag (2021:890) om skydd för personer som rapporterar om missförhållanden.

Sw. Förordning (2021:949) om skydd för personer som rapporterar om missförhållanden.

Local deviations or additional information in relation to the Whistleblower Directive

The applicable legal basis for processing of personal data will vary depending on the number of employees in the Swedish subsidiaries.

1. Swedish subsidiaries with at least 250 employees

For Swedish subsidiaries with at least 250 employees, the legal bases for processing of personal data will be as follows as from 17 July 2022:

- The processing is necessary for compliance with a legal obligation to which Viaplay Group is subject (GDPR Article 6.1 (c) and Chapter 2 Section 1 of the Act (2018:218) with supplementary provisions to the EU Data Protection Regulation.
- Any sensitive personal data is processed on the legal basis that it is necessary for reasons of substantial public interest (GDPR Article 9.2 (g)), or for the purposes of carrying out the obligations and exercising specific rights of Viaplay Group in the field of employment (GDPR Article 9.2 (b) and Chapter 3 section 2 of the Act (2018:218) with supplementary provisions to the EU Data Protection Regulation), as the case may be.
- Any personal data about criminal offences is processed on the basis of that the processing is necessary for compliance with a legal obligation (GDPR Article 10 and Section 5.2 of the Ordinance (2018:219) with supplementary provisions to the EU Data Protection Regulation).

2. Swedish subsidiaries with 50-249 employees

From 17 December 2023 and onwards:

- The legal bases for processing of personal data stated under section 1 above will apply also to Swedish subsidiaries with 50-249 employees.

Until 17 December 2023:

- For the period until 17 December 2023, the following legal bases will apply to Swedish subsidiaries with 50-249 employees, the processing is necessary for the purposes of the legitimate interests pursued by Viaplay Group (GDPR Article 6.1 (f). Viaplay Group's legitimate interest is to investigate concerns relating to whistleblowing incidents.
- Any sensitive personal data is processed on the legal basis that it is necessary for the establishment, exercise or defence of legal claims (GDPR Article 9.2 (f) or for the purposes of carrying out the obligations and exercising specific rights of Viaplay Group in the field

of employment (GDPR Article 9.2 (b) and Chapter 3 section 2 of the Act (2018:218) with supplementary provisions to the EU Data Protection Regulation), as the case may be.

- Any personal data about criminal offences is processed on the basis of that the processing is necessary for the establishment, exercise or defence of legal claims (GDPR Article 10 and Section 5.1 of the Ordinance (2018:219) with supplementary provisions to the EU Data Protection Regulation), as well as the Swedish Authority for Privacy Protection's regulation DIFS 2018:2.

3. Swedish subsidiaries with less than 50 employees

For Swedish subsidiaries with less than 50 employees, the legal bases stated under section 2 will apply.

External reporting channels provided by local authorities

(applicable as from 17 July 2022)

The Data Protection Authority (IMY):
- The area of privacy and personal data protection and security of network and information systems.

The Economic Crime Authority (Ekobrottsmyndigheten):
- The area of the EU's financial interests as regards the fight against fraud.

Financial Supervisory Authority (Finansinspektionen):
- The area of financial services, products and markets and the prevention of money laundering and terrorist financing.

The Public Health Agency of Sweden (Folkhälsomyndigheten):
- The area of public health in the production, presentation and sales of tobacco products and thereby related products.

The Social Insurance Agency (Försäkringskassan):
- The area of public health as regards patient rights.

The Agency for Marine and Water Management (Havs- och vattenmyndigheten):
- The area of environmental protection as regards the protection and management of water and land.
- The area of environmental protection as regards the protection of nature and biodiversity.

The Inspection for Strategic Products (Inspektionen för strategiska produkter):
- The area of product safety and conformity with regard to the marketing and use of sensitive and dangerous products.

The Board of Agriculture (Jordbruksverket):
- The area of food and animal feed safety and animal health and welfare, as regards animal health.
- The area of food and animal feed safety and animal health and welfare, as regards animal welfare standards and animal health and welfare.

The Chemicals Agency (Kemikalieinspektionen):
- The area of environmental protection as regards chemicals.

The Competition Authority (Konkurrensverket):
- The area of public procurement.
- The area of the internal market, as regards competition.

The Consumer Protection Agency (Konsumentverket):
- The area of consumer protection.

The Food Agency (Livsmedelsverket):

- The area of food and animal feed safety and animal health and welfare, as regards food and feed legislation.
- The area of food and animal feed safety and animal health and welfare, as regards public control and other public activities to ensure the application of food and feed legislation.
- The area of environmental protection in respect of organic products.

The Medical Products Agency (Läkemedelsverket):

- The area of public health as regards measures to establish high quality and safety standards for organs and substances of human origin.
- The area of public health as regards measures to establish high quality and safety standards for medicinal products and medical technology devices.

The Environmental Protection Agency (Naturvårdsverket):

- The area of environmental protection in respect of any criminal offence against the protection of the environment and infringements of the legislation set out in the Appendices to Directive 2008/99/EC.
- The area of environmental protection as regards the environment and climate.
- The area of environmental protection in terms of sustainable development and waste management.
- The area of environmental protection in the field of marine, air and noise pollution.

The Government Offices of Sweden (Regeringskansliet):

- The area of the internal market, as regards the state aid area.
- The area of EU financial interests, as regards the state aid area.

The Radiation Safety Authority (Strålsäkerhetsmyndigheten):

- The area of radiation protection and nuclear safety.

The Tax Agency (Skatteverket):

- The area of the internal market, as regards the area of corporation tax.
- The area of the EU's financial interests, as regards the area of taxation.

The Board of Accreditation and Technical Control (Swedac) (Styrelsen för ackreditering och teknisk kontroll):

- The area of product safety and conformity as regards general safety and conformity requirements for products released on the EU market.

The Transport Agency (Transportstyrelsen):

- The area of transport safety.

Appendix 3 - Denmark

Scope of applicability

This Appendix applies to whistleblowing taking place in Denmark.

Applicable local law

Lov 2021-06-29 nr. 1436 om beskyttelse af whistleblowere (Act 2021-06-29 No. 1436 on the protection of whistleblowers) (hereafter referred to as the Danish "Whistleblower Act")

Local deviations in relation to the Whistleblower Directive

GDPR

The applicable legal basis for processing of personal data will vary depending on the number of employees in the Danish subsidiaries.

1. Danish subsidiaries with at least 250 employees

For Danish subsidiaries with at least 250 employees, the legal bases for processing of personal data will be as follows as from 17 December 2021:

- The processing is necessary for compliance with a legal obligation to which Viaplay Group is subject (GDPR, Article 6.1 (c), the Data Protection Act section 6 (1) and The Whistle-blower Act section 22).
- Any sensitive personal data is processed on the legal basis that it is necessary for reasons of substantial public interest (GDPR, Article 9.2 (g), the Data Protection Act section 7 (4) and the Whistle-blower Act section 22), or for the purposes of carrying out the obligations and exercising specific rights of Viaplay Group in the field of employment (GDPR, Article 9.2 (b), the Data Protection Act section 7 (2) and the Whistle-blower Act section 22), as the case may be.
- Any personal data about criminal offences is processed on the basis of that the processing is necessary for compliance with a legal obligation (GDPR, Article 10, the Data Protection Act section 8 (3) and the Whistle-blower Act section 22).

2. Danish subsidiaries with 50-249 employees

From 17 December 2023 and onwards:

- The legal bases for processing of personal data stated under section 1 above will apply also to Danish subsidiaries with 50-249 employees as from 17 December 2023.

Until 17 December 2023:

For the period until 17 December 2023, the following legal bases will apply to Danish subsidiaries with 50-249 employees:

- The processing is necessary for the purposes of the legitimate interests pursued by Viaplay Group (GDPR GDPR, Article 6.1 (f) and the Data Protection Act section 6 (1). Viaplay Group 's legitimate interest is to investigate concerns relating to whistleblowing incidents.
- Any sensitive personal data is processed on the legal basis that it is necessary for the

establishment, exercise or defence of legal claims (GDPR, Article 9.2 (f) and the Data Protection Act section 7 (1) or for the purposes of carrying out the obligations and exercising specific rights of Viaplay Group in the field of employment (GDPR, Article 9.2 (f) and the Data Protection Act section 7 (1)), as the case may be.

- Any personal data about criminal offences is processed on the basis of that the processing is necessary for the establishment, exercise or defense of legal claims (GDPR, Article 10, and the Data Protection Act section 8 (3)), as well as the Danish Authority for the Data Protection Act section 8 (1).

3. Danish subsidiaries with less than 50 employees

For Danish subsidiaries with less than 50 employees, the legal bases stated under section 2 will apply.

What to report

According to the Danish Whistleblower Act it must be possible to report serious offenses or other serious matters - in addition to violations of certain areas of EU law, cf. section 3.1 of the Whistleblower Directive. Such serious offense can also be sexual harassment or gross harassment and bullying, for example.

In each individual case, it depends on a specific assessment whether the report can be regarded as a serious offense or a serious matter in general. This is an objective criterion, where it is ultimately up to the Danish courts to assess whether a report falls within or outside the scope of the law.

The scope generally includes information on criminal offenses, including breaches of any duty of confidentiality, misuse of financial means, theft, fraud, embezzlement, bribery, as well as gross or repeated violations of legislation, including legislation on the use of force, the Public Administration Act, the Public Access Act and such circumstances e.g., legislation aimed at ensuring public health, safety in the transport sector or protection of nature and the environment, etc., is covered.

Protection

According to the Danish Whistleblower Act the protection against reprisals also includes the following persons:

- Communicators
- Third parties who are connected to the whistleblower and who risk being subjected to reprisals in a work-related context.
- Companies and authorities that the whistleblower owns or works for or is otherwise associated with in a work-related context.

External reporting channels provided by local authorities

- Danish Data Protection Agency (Datatilsynet): https://whistleblower.dk/
- Danish Security and Intelligence Service (PET): www.jm.dk
- Danish Ministry of Defence (FE): www.fmn.dk
- Danish Financial Supervisory Authority (Finanstilsynet): https://www.finanstilsynet.dk/whistleblower

- Danish Business Authority (Erhvervsstyrelsen): https://erhvervsstyrelsen.dk/whistleblowerordning
- Danish Working Environment Authority Danish (Arbejdstilsynet): https://offshore.at.dk/whistleblower/.
- Danish Environmental Protection Agency (Miljøstyrelsen): https://mst.dk/erhverv/industri/olie-og-gasproduktion-i-nordsoeen-offshore/

Appendix 4 – Document History and Change Information

Version	Revision Date	Change Information
1	2018-10-10	Initial Group Directive.
2	2019-12-13	New Document Owner and Whistleblower officers due to internal reorganisation. New reference to Viaplay Group 's Reporting an
2.1	2020-06-25	Change of Data controller due to Expolink being acguired by Navex Global (Appendix 1). Adding contact details to our DRO (Appendix 1) as well as minor linguistic changes and clarifications of the text.
3	2020-11-26	Change in p. 5 "Transfer of personal data" due to the Privacy shield mechanism no longer being valid.
4	2022-09-09	Major changes to content as a result of the EU Whistle-blower Directive and employer's and employee's rights and obligation
5	2023-10-17	Editorial changes.
6	2024-10-15	Editorial changes.
7	2025-12-01	Comprehensive linguistic and structural clarifications to improve readability and consistency; clarified scope, target groups and definitions of reportable matters; refined descriptions of internal and external reporting channels, confidentiality and non-retaliation; aligned wording mor closely with applicable whistleblowing and data protection legislation without changing underlying rights and obligations.