Group Whistle-blower Directive

Document owner	Head of Group Compliance
Approval	CEO/CFO
Initially adopted	10 October 2018
Date last approved	December 2023
Date of next review/approval	Q4 2024
Applicability	Group

viaplay GROUP

Whistleblower Directive

1. *Introduction*

Viaplay Group AB (Viaplay Group) seeks to conduct business with responsibility, honesty, and integrity at all times, and we expect our people to do the same. 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 Viaplay Group to know that their concerns will be taken seriously and investigated properly without fear of retaliation, and that their confidentiality will be respected.

2. *Target Group*

This directive applies to all individuals working at all levels of Viaplay Group. This includes senior executives, managers, directors, employees (whether permanent, fixed-term, or temporary), job seekers, consultants, contractors, interns, and other people who, in a work-related context, have a relationship with us ("Workers") in all subsidiaries and entities in which Viaplay Group exercises decisive control (directly or indirectly) and is to be used on a voluntary basis. The same applies to parties such as employees of partners with whom Viaplay Group has an established work relationship. The Directive also applies to persons who had a work-related relationship with us that has ended, and received or obtained information during that time in the business.

3. *Principles and Procedures*

3.1. What should I report in the whistleblowing service?

The whistleblowing service allows you to report witnessed or suspected misconduct in a work-related context that has happened or is very likely to happen and for which there is a public interest.

Instances of misconduct that warrant disclosure in the interest of the public generally involve actions and omissions that violate regulations or laws. The whistleblowing service is also designed to receive reports concerning suspicions regarding actions or omissions that violate directly applicable European Union laws as defined in the EU Whistleblowing Directive[1], or that violate regulations implementing or supplementing such laws. .[2]

Directly applicable European Union law acts exist, for example, within the following areas: public procurement; financial services; products and markets; and the prevention of money launderingand terrorist financing; environmental protection; public health; consumer protection, and privacy and personal data protection; as well as security of network and information systems.

In line with the above, certain acts or omissions contrary to Viaplay Group 's Code of Conduct or Supplier & Business Partner Code of Conduct, such as anti-corruption, competition, sanction

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

compliance, intellectual property, data protection, and information security matters, would also fall under the scope of this directive.

Please note that information relating soleyto your own working or employment relationship is normally not of such nature that it is of a public interest. Hence, such information is covered only in exceptional circumstances, such as situations involving labour exploitation of minors or conditions resembling slavery. Another example is an employer's systematic violations of applicable regulations in relation to an employee. See Section 3.2, which further specifies what information should not be reported through this whistleblowing service.If you are unsure whether or not an issue qualifies as a whistle-blowing concern, please seek advice from Viaplay Group 's Whistleblowing Officers.

Anyone who submits a report should be honest. No accusations may be made with malicious intent or knowing that the allegation is false. We take abuse of the system seriously.

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

If your concerns relate to the work environment, minor misconduct, concerns relating to poor management, difficulties in cooperating with people, workplace dissatisfaction, inefficient systems, or other operational feedback, then you should follow 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. The same applies for concerns relating to your terms and conditions of employment. Openness makes it easier for Viaplay Group to assess and investigate the matter.

However, special cases concerning gross personal misconduct that gives rise to a crime, such as, for example, modern slavery, human trafficking, child labour, and similar, should be reported using the whistle-blowing channels. See also Appendix 3 for Denmark in case the violation you want to report concerns those operations, as specific rules apply.

3.3. How should I report?

If you observe conduct that you believe falls within the scope of this Whistleblower Directive (i.e. in accordance with section 3.1 above), we encourage you to report it using one of the internal channels described below:

- **Option 1: Report on a group level via Viaplay Group's Speak-Up Line :** You may submit a written or oral account of the concern or request a virtual or in-person meeting through Viaplay Group's joint whistleblowing channel – the Speak-Up Line. Your report will be forwarded to one of the Group's whistleblower officers to facilitate additional communication and inquiry.

- Please refer to Appendix 1 – internal Reporting and Data Protection, Section 3 for more information regarding how our Speak-Up Line works.

- **Option 2: Report locally via local whistle-blower channel (Currently, only avaliable for reporting violations concerning operations of Viaplay Group Sweden AB):** You may submit a written or oral account of the concern or request 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 variations from the provisions outlined in this directive, kindly consult 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 come forward.

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

3.4. External reporting and local rules

Reporting to an authority

In addition to internal reporting, it is also possible to report a misconduct that falls within the scope of this directive (i.e., in accordance with Section 3.1 above) externally to a competent authority in an EU country. The authority's reporting channels are independent in relation to the authority's other activities.

For comprehensive information regarding local variations from the provisions outlined in this directive, kindly consult Appendix 2 (Sweden) or Appendix 3 (Denmark).

Please note that if you report externally to a competent authority in any other way than through that authority's external reporting channel, certain requirements apply. You must either i) have reported internally without the recipient taking sufficient action or providing feedback within three months from the report; ii) have reasonable grounds to believe that the misconduct constitutes an imminent or obvious danger to life, health, safety, or risk of extensive damage to the environment, or for any other valid reason to report to the authority; or iii) have reasonable grounds to believe that internal reporting would entail a risk of retaliation or that the misconduct would not be remedied effectively.

In the case of external reporting, 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.

Reporting to EU institutions, bodies or agencies

If the subject-matter of the report concerns the competence of an EU institution, body, or agency, it is also possible to report to them through their external reporting channels.

Local rules

Local laws and regulations in the countries where Viaplay Group conducts its business may contain rules that deviate from or supplement 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 comprehensive information regarding local variations from the provisions outlined in this directive, kindly consult Appendix 2 (Sweden) or Appendix 3 (Denmark).

3.5. Confidentiality and Non-Retaliation

Viaplay Group will take all reasonable steps to ensure confidentiality throughout the reporting process. Workers filing unanonymous (open) reports should not fear that their identity will be improperly disclosed or abused. The Whistleblower Officers are bound by confidentiality, ensuring the confidential handling of whistleblowing cases. 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.

The person handling a case following up a reporting may not without authorization disclose information that may reveal the identity ofindividuals in the case. This means that Viaplay Group will not disclose your identity outside the investigation team. However, in some cases information can be considered duly disclosed and thereby not be subject to confidentiality. Information that is transferred to other Viaplay Group entities for action as a result of conclusions reached during the follow-up of the reporting information is one example.. Personal data provided via an internalwhistleblowing report will be processed in accordance with the principles outlined in Appendix 1 “Internal reporting and data protection”.

Viaplay Group strictly forbids any 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 turns out to be inaccurate or does not trigger any 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 expresses an intention to do so, will not be tolerated. Workers involved in such conduct may face 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 whistle-blowing channel.

Please note that making deliberately false, unfounded or malicious allegations may result in disciplinary action, up to and including dismissal.

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

3.6. The process – internal reporting

Step 1: Assessment (you)

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

Step 2: Preparation (you)

- You can choose whether to report anonymously or to state your identity. If possible, we recommend you gather evidence and information. However, this is not a requirement. The more supporting material you provide in your report, the easier it is for us to investigate and substantiate your claims. Precise dates, including a precise description of the breach, names of people involved, possible witnesses, and evidence such as documents and e-mails, etc. will all assist Viaplay Group in investigating the matter.
- We do not require you to offer a specific level of proof when reporting a matter, but you must reasonably believe the information is substantially true.
- When making your report, please be aware that the information you provide or the allegations that you make could result in decisions that affect Viaplay Group Workers. We therefore kindly ask that you provide us with information that is accurate to the best of your knowledge. In addition, try to only provide information that is adequate, relevant, and necessary to handle and investigate your allegations.
- Irrelevant privacy information – that is offensive, such as non-relevant information about health status, political or religious affiliation, or sexual orientation, shall not be included in a report.

Step 3: Receipt of report (Viaplay Group)

- If a concern is raised, it will be assessed by Viaplay Groups Whistleblower Officers to determine whether it falls under the scope of this directive. If the report is approved, appropriate investigative measures are taken (see step 4 below).
- The Whistleblower Officers will refuse to receive a report if the report does not fall within the scope of what can be reported through the whistleblowing service (see Section 3.1 and 3.2 above) or if the report has not been made in good faith.
- The Whistleblower Officers may refuse to receive a report if there is not enough information to investigate the case or if the case to which the report relates has already been addressed.
- The Whistleblower Officers are responsible for the correct handling of reports. If a report does not fall within the scope of what is to be investigated as a whistleblowing case, the Whistleblower Officers will notify you (provided that it is possible). If the report is of a HR nature, the concern will usually be passed to local HR for further handling or investigations.
- If an oral report is documented through a transcript or minutes from a meeting, you will be given the opportunity to check, rectify, and agree to the content by signing it.

Step 4: Investigation (Viaplay Group)

- For reports that fall under the scope of this directive they will be assessed by Viaplay Group's Whistleblower Officers to decide whether there is enough

information to warrant an in-depth investigation. If so, adequate actions will be taken for further investigation. If not, then one of the Whistleblower Officers may revert to you for further information. By which means the Whistleblower Officers revert to you depends on whether you revealed your contact information or not when you reported.

- The Whistleblower Officers are required to handle the whistleblowing reports with confidentiality and ensure that a report is not investigated by anyone affected by or involved in the case.

  If an investigation is initiated, a Whistleblower Officer will inform you, where possible. This may include a request for an interview or for further information. The Whistleblower Officer may inform you of a wider investigation with other affected parties, which may include contacting the person against whom allegations have been raised. Which means the Whistleblower Officer informs you depends on whether you revealed your contact information or not when you reported. If you choose to report anonymously, any follow up questions and requests for additional information will be provided through the Speak-Up Line.

Step 5: Communication (Viaplay Group)

- Confirmation that a report has been received will be provided to you within seven days of receipt.
- The Whistleblower Officer will, within three months from the confirmation of receipt of the report, provide feedback to a reasonable extent on the measures taken in the follow up of the report and on the reasons for this.
- 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.
- Thereafter you will be informed to a reasonable extent of the progress of the investigation.
- If a decision is taken to end the investigation for whatever reason, this decision will be communicated to you.
- Once the investigation has been completed, feedback will be communicated to you. If the report has been provided anonymously, the feedback will be provided through the Speak-Up Line or the means by which communication was established by the individual.

Step 6: Action (Viaplay Group)

If the concern raised is found to be valid, then Viaplay Group may decide that one or more of the following steps is appropriate (this list is not exhaustive):

- action taken as appropriate to address the concern raised; or
- referral of the matter to the Chairman of Viaplay Group 's Audit Committee; or
- referral of the matter to Viaplay Group 's Board of Directors; or
- referral of the matter to the appropriate external regulatory body; and/or
- referral of the matter to the police.
- Viaplay Group furthermore reserves the right to check in on the reporter within a couple of months after the case has been closed in order to ensure that the person has not been

retaliated. If a reporter feels like they have been retaliated against in connection with filing the report, they should file this retaliation case separately in the whistle-blowing channel.

3.7. Further information

For further information regarding our use of personal data, please see Appendix 1. For further information on whistle-blowing, visit the Business Ethics site on ViaPLACE.

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

4. *Roles and Responsibilities*

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

The individual is responsible for maintaining & updating the Directive, and for ensuring that it is properly published and enforced. The individual is also responsible for making sure this Directive is communicated to and implemented by Workers whom it may affect.

5. *References*

Internal reporting and data protection, Appendix 1.

6. *Document History and Change Information*

For more details of this Group Directive's document history and change information, see Appendix 4.

Appendix 1 - Internal Reporting and Data Protection

1. Privacy Statement

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 's 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@viaplay group.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.

viaplay GROUP

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.

Any 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

2.1 As 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 as from 17 December 2023.

2.2 For the period 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

With respect to Swedish subsidiaries with less than 50 employees, the legal bases stated under section 2.2 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.

viaplay GROUP

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")

Any 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

2.1 As 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.

2.2 For the period 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

With respect to Danish subsidiaries with less than 50 employees, the legal bases stated under section 2.2 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:

1) Communicators

2) Third parties who are connected to the whistleblower and who risk being subjected to reprisals in a work-related context.

3) 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/

viaplay GROUP

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 Incident
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-	Major changes to content as a result of the EU Whistle-blower Directive and employer’s and employee’s rights and obligation thereof.
5	2023-10-17	Editorial changes.