Embracer Group Whistleblowing Guidelines

Adopted by Embracer Group Chief of Staff, Legal & Governance on 12 September 2023
Revised:
Document type: Guidelines
Version: 1
Document owner: Embracer Group Head of Governance & Compliance

These Guidelines apply to the Embracer Group entities and all employees in Embracer Group.

These Guidelines expand and detail the Whistleblowing routine and tool within Embracer Group. Local level guidelines can exist in parallel with these Guidelines to supplement with local legal requirements or processes.

If you have any questions about these Guidelines, please contact:
Embracer Group Head of Governance & Compliance, Legal

Embracer Group Whistleblowing Guidelines

Table of Content

1. Revision history

Date	Version	Description	Author
2023-09-12	1.0	First version adopted by Embracer Group Chief of Staff, Legal & Governance	Head of Governance & Compliance

2. Introduction - what is whistleblowing, and why is it important?

2.1 Our organisation strives to achieve transparency and a high level of business ethics. Embracer Group AB and its entities ("Embracer Group") has zero tolerance for acts such as discrimination, harassment, crime, corruption and environmental crime. Equal treatment of all employees in Embracer Group ("Employees"), customers and suppliers as well as good business ethics is a key element. These core values have been documented in our Code of Conduct and our Supplier Code of Conduct. The codes describe Embracer Group's principles and approach for Employees and business partners, and for Embracer Group as an employer and member of the community.

2.2 Embracer Group encourages its Employees, business partners, suppliers and other external contacts to notify Embracer Group/ the organisation if they have identified a serious problem or have serious suspicions of fraud, corruption, harassment or similar irregularities within the Group's operations. The Employees, and also third parties have an important role in giving notice if they suspect something that is contrary to Embracer Group's Code of Conduct/ Supplier Code of Conduct. This gives Embracer Group/ the organisation an opportunity to prevent but also correct if something has gone wrong. Our whistleblowing service offers a possibility to alert Embracer Group/ the organisation about suspicions of misconduct in a confidential way. It is an important tool for reducing risks and maintaining trust in our operations by enabling us to detect and act on possible misconduct at an early stage. Whistleblowing can be done by any person openly or anonymously.

2.3 The purpose of these Guidelines is partly to inform about our internal reporting channels and how reporting and follow-up of reports takes place, and partly to ensure that we fulfil our obligations according to the Directive [EU] 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union Law and applicable rules on data protection ("the Whistleblowing Directive") as well as any specific local requirements in the EU Member States where we operate. These Guidelines apply to all Employees, contractors, interns, job applicants and others who perform or have performed work for and under the management of Embracer Group in the European Union.

3. When to blow the whistle?

3.1 The whistleblowing service can be used to report any breaches falling within the following areas (the "In-Scope areas"), which are:

1. Breaches of European Union law falling within the material scope of the Whistleblowing Directive including:

- Breaches falling within the scope of the Union acts set out in the Annex to the Whistleblowing Directive that concern the following areas:
    - Public procurement;
    - Financial services, products and markets, and prevention of money laundering and terrorist financing;
    - Product safety and compliance;
    - Transport safety;
    - Protection of the environment;
    - Radiation protection and nuclear safety;
    - Food and feed safety, animal health and welfare;
    - Public health;
    - Consumer protection;
    - Protection of privacy and personal data, and security of network and information systems.
- Breaches affecting the financial interests of the European Union as referred to in Article 325 TFEU and as further specified in relevant Union measures; and
- Breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

2. Any other Breach in the areas prescribed by national laws as further listed in the relevant Country-specific Appendices below.

3.2 Employees are asked to contact their HR supervisor, manager or local Compliance Officer or function for issues relating to dissatisfaction in the workplace or related matters, as these issues cannot be investigated in the scope of whistleblowing.

3.3 A person who blows the whistle does not need to have firm evidence for expressing a suspicion. However, deliberate reporting of false or malicious information is forbidden. Abuse of the whistleblowing service may constitute a disciplinary offence, which may lead to disciplinary actions, up to termination, subject to local law.

3.4 Please note that the scope of reportable breaches may be wider in certain countries and that there may be specific provisions and requirements for the use of a whistleblowing service. Please see more information on https://report.whistleb.com/embracer – where country specific provisions will be shown when choosing your language and in the country specific appendices to these Guidelines, **Appendices A-N**.

4. How to blow the whistle?

4.1 There are different ways to raise a concern:

- **Alternative 1:** Contact a HR supervisor, manager or local Compliance Officer or function within our organisation.
- **Alternative 2:** Contact:

  Embracer Group AB, Chief of Staff, Legal & Governance, Ian Gulam

  Phone: +46 72 857 70 17 Email: ian.gulam@embracer.com

  A report may also be made by means of a physical meeting. If an employee requests a physical meeting, the meeting will take place within a reasonable time in accordance with local law.
- **Alternative 3:** Anonymous or confidential messaging through the Group whistleblower reporting channel to the whistleblowing team: https://report.whistleb.com/embracer.
- **Alternative 4:** Reporting to external channels maintained by competent authorities or, where applicable, EU institutions, bodies or agencies through their external reporting channels. External reporting to a certain authority can be done provided that the misconduct falls within the jurisdiction of the competent authority. When reporting externally, it is the relevant authority who is responsible for receiving the report, provide necessary information and follow-up. Further information about reporting externally is set out in the country specific appendices to these Guidelines.

4.2 We offer a choice of reporting to the Group channel operated by Embracer Group HQ (Alternative 3), or to report at local Operative Group/ subsidiary level using the channels available on https://report.whistleb.com/embracer. Reports via subsidiary channels are managed by representatives of that legal entity.

4.3 All messages received will be handled confidentially. For those wishing to remain anonymous, we offer channels for anonymous reporting. The whistleblowing channels enabling anonymous messaging are administrated by WhistleB, an external service provider. All messages are encrypted. To ensure the anonymity of the person sending a message, WhistleB deletes all meta data, including IP addresses. The person sending the message also remains anonymous in the subsequent dialogue with responsible receivers of report. Reports may be submitted via the dedicated web page https://report.whistleb.com/embracer from any device and in any language or by telephone (optional service), in which case the reporter can call and leave a secure recorded voice message via our telephone answering service provided by WhistleB. Local phone numbers and additional instructions can be found on https://report.whistleb.com/en/message/embracer/phone.

4.4 Please note there could be country specific requirements and restrictions on the use of a whistleblowing service in certain countries. Please see more information on https://report.whistleb.com/embracer – where specific restrictions will be

shown when choosing your language and in the Country Specific appendices to these Guidelines, Appendices A-O.

5. The investigation process

5.1 The whistleblowing team

5.1.1 Access to messages received through our whistleblowing channels is restricted to appointed individuals at Embracer Group AB (the parent company) or at each local Operative Group/ subsidiary level with the authority to handle whistleblowing cases. Their actions are logged and handling is confidential. When needed, individuals who can add expertise may be included in the investigation process, upon consent from the whistleblower in case identity of the reporting person is disclosed. These individuals can access relevant data and are also bound to confidentiality.

5.1.2 If a person raises a concern directly to a HR supervisor, manager, local Compliance Officer or function or by contacting the whistleblowing team in person the message is treated according to these Guidelines.

5.2 Receiving a message

5.2.1 Upon receiving a message, the whistleblowing team decides whether to accept or decline the message. If the message is accepted, appropriate measures for investigation will be taken, please see section 5.3 Investigation below.

5.2.2 The whistleblower will receive an acknowledgment of receipt of the report within seven (7) days.

5.2.3 The whistleblowing team may not investigate the reported misconduct if:

- the alleged conduct is not reportable conduct under these Whistleblowing Guidelines
- the message has not been made in good faith or is malicious
- there is insufficient information to allow for further investigation
- the subject of the message has already been solved

5.2.4 If a message includes issues not covered by the scope of these Whistleblowing Guidelines, the whistleblowing team should provide the reporting person with appropriate instructions.

5.2.5 The whistleblowing team will send appropriate feedback within three (3) months upon the date of receiving the report.

5.2.6 Do not include sensitive personal information about anyone mentioned in your message unless necessary for describing your concern.

5.3 Investigation

5.3.1 All messages are treated seriously and in accordance with these Whistleblowing Guidelines.

- No one from the whistleblowing team, or anyone taking part in the investigation process, will attempt to identify the whistleblower.

- The whistleblowing team can, when needed, submit follow-up questions via the channel for anonymous communication.
- A message will not be investigated by anyone who may be involved with or connected to the wrongdoing.
- The whistleblowing team decides if and how a whistleblowing message should be escalated.
- Whistleblowing messages are handled confidentially by the parties involved.

6. Protection and Privacy

6.1 Whistleblower protection

6.1.1 A person expressing genuine suspicion or misgiving according to these Guidelines will not be at risk of losing their job or suffering any form of sanctions or personal disadvantages as a result. It does not matter if the whistleblower is mistaken, provided that he or she is acting in good faith.

6.1.2 Subject to considerations of the privacy of those against whom allegations have been made, and any other issues of confidentiality, a whistleblower will be kept informed of the outcomes of the investigation into the allegations.

6.1.3 In cases of alleged criminal offences, the non-anonymous whistleblower will be informed that his/her identity may need to be disclosed during judicial proceedings.

6.2 Archiving of report and handling of personal data

6.2.1 Regardless of whether your report is received directly by the Whistleblower function or via another channel, the information collected is transferred to the Whistleblower function for follow-up and archiving. This is to ensure maximum protection for your data and to ensure that your data is cleared correctly.

6.2.2 The personal data included in the reported case is processed with the legal basis of legal obligation to be able to receive, investigate and act on your report and take any measures connected to this. The personal data is processed while the case is ongoing and for a period of twelve (12) months after the case has been archived unless applicable legislation specifies a different storage period. This is to be able to follow up on cases after completion and to be able to re-open cases if this is required due to legislation or the circumstances of the case.

6.2.3 When your personal data is processed because of a legal obligation you have the right to have your personal data corrected and to access it.

6.2.4 If you have questions about the processing of personal data or if you want to exercise any of your rights, you are welcome to contact Embracer Group AB's data protection officer at dpo@embracer.com. You also have the right to complain about the processing of personal data to your local supervisory

authority, which in Sweden is IMY, the Swedish supervisory authority for personal data. www.imy.se.

7. Appendices

Appendices A-N – Country Specific Appendices

EMBRACER GROUP

Appendix A – Country Specific Provisions – Austria

Application of the Guideline (Personal Scope)

In specification of section 2.3 of the Whistleblowing Guidelines, these Guidelines apply to current or former:

1. employees and leased employees (temporary workers),
2. job candidates, interns, apprentices, trainees, volunteers,
3. self-employed workers, freelancers, consultants, service providers,
4. shareholders, directors, members of a supervisory board or other boards,
5. contractors, subcontractors and suppliers, and anyone working under the supervision of them.

Reporting Concerns (Material Scope)

These Guidelines apply to reporting such misconducts that fall within the material scope of the Austrian Whistleblowing Act ("*HinweisgeberInnenschutzgesetz – HSchG*", BGBl. I Nr. 6/2023), which are the following:

1. Misconducts in breach of the European Union law falling within the scope of the Whistleblowing Directive as set out in section 3.1 of the Whistleblowing Guidelines (the "**Scope**") above;
2. Misconducts in breach of Austrian law that relate to the Scope, even if implemented without a link to the laws of the European Union;
3. Reports relating to the prevention and punishment of criminal offenses under sections 302 to 309 of the Austrian Criminal Code ("Strafgesetzbuch – StGB", BGBl. Nr. 60/1974), relating to the violation of official duties, corruption, bribery and related criminal acts.

Freedom to raising a Concern

In addition to the possibilities of reporting in writing or orally as set out in section 4.1 of the Whistleblowing Guidelines, you can also request a personal meeting to discuss your report. The face-to-face meeting will take place within 14 days after your request.

Receiving a message

Any message received, will be accepted. The whistleblowing team decides whether to launch an investigation based on the message.

Where messages are reported orally, including over a telephone line, the oral message may be recorded by audio recording or by complete and accurate recording of the message with transcription of the conversation, provided you give your consent.

Whistleblower protection

In cases of alleged offences, the non-anonymous whistleblower will be informed that his/her identity may need to be disclosed during judicial or administrative proceedings.

External Reporting Channels

In Austria, internal reporting is the preferential channel to report concerns related to the above mentioned issues. You may also report a breach externally, but before you report externally, you should check whether a report can be made internally.

Only if an internal report is not possible, appropriate or reasonable, or you tried to report internally and it has proven to be unsuccessful or futile, you should report externally.

You can find the competent authorities below (note that the list is not exhaustive and may evolve). Information on how to report can be found on the respective authority's website.

Federal Office for the Prevention of and Fight against Corruption ("*Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung*")

The Federal Office for the Prevention of and Fight against Corruption is the external reporting office for all reports of misconducts falling within the Scope, unless the misconduct falls within the specific competencies of one of the authorities listed below.

If there is a specific competence and the report was nevertheless submitted to the Federal Office for the Prevention of and Fight against Corruption, the report will automatically be forwarded to the competent authority and you will be informed about the forwarding.

Information on how to report can be found on the following website: https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=8HObc4&c=-1&language=ger

Auditors' Oversight Authority ("*Abschlussprüferaufsichtsbehörde*")

You can report to the Auditors' Oversight Authority if you have information about violations of provisions of the Auditor Oversight Act or other provisions relevant to the audit of financial statements.

Information on how to report can be found on the following website: https://www.apab.gv.at/aufsicht/whistleblower

Balance Sheet Accounting Authority ("*Bilanzbuchhaltungsbehörde*")

The Balance Sheet Accounting Authority receives reports of non-compliance with the duties to prevent money laundering and terrorist financing of authorized professionals within the authority's area of responsibility.

Information on how to report can be found on the following website: https://report.whistleb.com/de/bilanzbuchhaltung

Federal Competition Authority ("*Bundeswettbewerbsbehörde*")

If you discover violations in the area of competition, such as formation of a cartel or abuse of market power, you can report it to the Federal Competition Authority.

Information on how to report can be found on the following website: https://report.whistleb.com/de/bwb

Financial Market Authority ("*Finanzmarktaufsichtsbehörde*")

You can report to the Financial Market Authority if you have information of abuses or violation of supervisory law in an organization that is subject to the supervision by the Financial Market Authority (e.g., banks, insurance companies, pension funds).

Information on how to report can be found on the following website: https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=11FMA61&c=-1&language=ger

Money Laundering Reporting Center ("*Geldwäschemeldestelle*")

The Money Laundering Reporting Center receives information from professional groups subject to reporting requirements about transactions or business cases for which there are reasonable grounds to assume that they are related to money laundering or terrorist financing.

Information on how to report can be found on the following website: https://www.bundeskriminalamt.at/308/start.aspx

Chambers of Public Notaries ("*Notariatskammern*")

If you suspect that a member of the Chamber of Public Notaries is violating the provisions of the Notarial Code ("*Notariatsordnung – NO*") that serve to prevent or combat money laundering or terrorist financing, then you can file a report with the Chambers of Public Notaries.

Information on how to report can be found on the following website: https://report.whistleb.com/de/notar

Bar Associations of Lawyers ("*Rechtsanwaltskammern*")

You can report violations of the provisions of the Regulations for the Lawyers' Profession ("*Rechtsanwaltsordnung – RAO*") that serve to prevent or combat money laundering or terrorist financing to the Bar Associations of Lawyers.

Information on how to report can be found on the following website: https://www.oerak.at/hinweisgebersystem/?referrer=w

Chamber of Tax Advisors and Auditors ("*Kammer der Steuerberater und Wirtschaftsprüfer*")

Violations of the measures for the prevention of money laundering and terrorist financing which falls within the area of responsibility of the Chamber of Tax Advisors and Auditors can be reported to the Chamber.

Information on how to report can be found on the following website: https://report.whistleb.com/de/ksw

Head of the Federal Disciplinary Authority ("*Leiterin oder der Leiter der Bundesdisziplinarbehörde*")

You can report to the Head of the Federal Disciplinary Authority if you have information on violations of the law relating to the Federal Ministry of the Interior, including its subordinate departments.

Information on how to report can be found on the following website: https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=Dxuw3U&c=-1&language=ger

Appendix B – Country Specific Provisions – Belgium

Introduction

The Embracer Group Whistleblowing Guidelines fully apply to all employees of APPEAL STUDIOS SA, ASMODEE BELGIUM NV and REPOS PRODUCTION SPRL in Belgium. The different ways to raise a concern are outlined in detail in the body of these guidelines. They provide a safe channel to report breaches without fear of retaliation in order to strengthen the compliance and information culture.

External Reporting Channels

The Embracer Group strongly encourages reports to be made internally, so that any concerns can be resolved effectively. However, should you wish to report externally, in Belgium, you may also report misconducts with respect to the In-Scope areas listed above, as well as the fight against tax fraud and social fraud, using the external reporting lines maintained by the competent authorities listed below. However, the competence of the authorities varies, and more information on this and on how to report can be found on the respective authority's website:

- the Federal Coordinator;
- the Federal Public Service Economy;
- the Federal Public Service Finance;
- the Federal Public Service Public Health, Food Chain Safety and Environment;
- the Federal Public Service Mobility and Transportation;
- the Federal Public Service Employment, Labour and Social Dialogue;
- the Programming Public Service for Social Integration, Poverty Reduction, Social Economy and Metropolitan Policy;
- the Federal Agency for Nuclear Control;
- the Federal Agency for Medicines and Health Products;
- the Federal Agency for the Safety of the Food Chain;
- the Belgian Competition Authority;
- the Data Protection Authority;
- the Financial Services and Markets Authority;
- the National Bank of Belgium;
- Belgian Audit Oversight Board;
- the authorities mentioned in Article 85 of the law of September 18, 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash;
- the National Committee for the Security of Drinking Water Supply and Distribution;
- the Belgian Institute for Postal Services and Telecommunications;
- the National Institute for Health and Disability Insurance;
- The National Institute for the Social Security of the Self-employed;
- the National Employment Office;
- the National Social Security Office;
- the Social Intelligence and Investigation Service;
- the Autonomous Anti-Fraud Coordination Service; and
- the Shipping Control.

Contact person

If you have any questions about the Embracer Group Whistleblowing Guidelines or if you need assistance, please contact:

Name: Ian Gulam

Phone: +46 72 857 70 17

Email: ian.gulam@embracer.com.

EMBRACER GROUP

Appendix C – Country Specific Provisions – Bulgaria

Reporting Concerns

These Guidelines apply to reporting such misconducts that threaten or harm the **public interest** and the European Union law and that fall within the material scope of the Bulgarian Whistleblowers Protection Act (*Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения*) (the "**Act**"), which are the following:

1. Misconducts in breach of European Union and Bulgarian law falling within the scope of the Whistleblowing Directive as set out in Section 3.1 in the Whistleblowing Guidelines (the "**Scope**") above;

2. A committed criminal offence of a general nature of which the whistleblower has become aware in connection with the performance of their work;

3. Misconducts in breach of Bulgarian law that concern the following areas:
   - the rules for payment of outstanding public state and municipal claims;
   - the labour law rules;
   - the legislation related to the performance of public service.

The following types of breaches fall outside the material scope of the Act:

1. Breaches of public procurement rules involving defence or national security aspects covered by Article 346 of the TFEU;

2. Breaches of the protection of classified information within the meaning of the Bulgarian Classified Information Protection Act;

3. Breaches that have become known to persons exercising legal profession and for whom there is a legal duty to comply with the professional secrecy;

4. Breaches of the confidentiality of health information as defined in the Bulgarian Health Act;

5. Breaches of the secrecy of a court meeting;

6. Breaches of the rules of criminal proceedings.

Who may blow the whistle?

Reports that fall within the material scope of the Act may be submitted by the following persons that have become aware of a breach during or in connection with the performance of their employment or official duties or in any other **work-related context**:

1. a worker, a civil servant or another person who is employed, regardless of the nature of the work, the manner of pay and the source of the funding;

2. a person who works without an employment contract and/or is a freelance worker and/or a craft worker;

3. a volunteer or an intern;

4. a partner, a shareholder, a sole owner of the capital, a member of the management or supervisory body of a commercial company, a member of the audit committee of an enterprise;

5. a person who works for a natural or legal person, its subcontractors or suppliers;

6. a job applicant who has obtained information on a breach in this capacity;

7. a worker, where the information has been obtained in the framework of an employment or service relationship, which has been terminated at the time of the reporting;

8. any other whistleblower who reports a breach that they become aware of in a work-related context.

How to blow the whistle?

For reports that do not fall within the material scope of the Act or do not concern a Bulgarian entity, you may raise a concern as set out in section 4.1 in the Whistleblowing Guidelines.

For reports that fall within the material scope of the Act, there are different ways to raise a concern:

1. **Alternative 1:** Contact the employee responsible for receipt, registration and investigation of reports filed with the respective Bulgarian Embracer subsidiary.

   For Deca Games EOOD, the relevant contact details are as follows:

   - Name: Borislav Milkov
   - Phone: +35 988 619 28 27
   - Email: bobby@decagames.com
   - Address: 16A Angel Karaliychev str., Veliko Tarnovo 5000, Bulgaria
   - Meeting in person, within an appropriate timeframe as agreed between you and the responsible employee.

2. **Alternative 2:** Confidential messaging through the Group whistleblower reporting channel to the employee responsible for receipt, registration and investigation of reports filed with your employer: https://report.whistleb.com/embracer.
3. **Alternative 3:** Reporting to the external channel managed by the Bulgarian Commission for Personal Data Protection. Reports to the Commission may be filed in one of the following ways:

   - **In writing**: by email at whistleblowing@cpdp.bg; by post to: Sofia 1592, bul. "Prof. Tsvetan Lazarov" 2
   - **Orally**: on-site at the Commission for Personal Data Protection at: Sofia 1592, bul. "Prof. Tsvetan Lazarov" 2

Additional information on external reporting can be found on the Bulgarian Commission for Personal Data Protection's website https://www.cpdp.bg/?p=sub_rubric&aid=285.

Anonymous reporting is not permitted for Bulgaria. Proceedings will not be initiated on anonymous reports that fall within the material scope of the Act.

Reports must contain at least the following information:

1. the sender's three names, address and telephone number, as well as an email address, if any;

2. the names of the person against whom the report is filed and their workplace, if the report is filed against specific persons and they are known;

3. specific details of an actual or potential breach, the place and time of the breach, if already committed, a description of the act or the situation and other circumstances, as far as these are known to the whistleblower;

4. date of submission of the report;

5. signature, electronic signature or other identification of the sender.

To ensure that all locally specific requirements regarding the content and form of the report are complied with, we recommend using the reporting template approved by the Commission for Personal Data Protection. The template may be accessed on the website of the Commission on the following address:

https://www.cpdp.bg/?p=sub_rubric&aid=282 (in Bulgarian)

https://www.cpdp.bg/en/index.php?p=sub_rubric&aid=282 (in English)

Archiving of reports

Reports that fall within the material scope of the Act and any attached documents, including the subsequent documentation related to their investigation, shall be kept for a period of 5 years after the respective case is closed, except where there are criminal, civil, labor law and/or administrative proceedings in connection with the submitted report whereby the 5-year retention period shall begin after the official proceedings are completed.

Appendix D – Country Specific Provisions – Cyprus

The scope of the Whistleblowing Guidelines

The present Whistleblowing Guidelines apply to reporting such misconducts that fall within the material scope of the Law providing for the Protection of Persons Reporting Breaches of Union and National Law (Law 6(I)/2022) (the "**Cypriot Whistleblower Act**") which implements the EU Whistleblower Directive.

The In-Scope areas as set out in section 3.1.2 of the Whistleblowing Guidelines may also be reported through the whistleblowing service, pursuant to the provisions of the Cypriot Whistleblower Act:

1. Acts or omissions relating to the commission or possible commission of a criminal offence, in particular corruption offences;

2. Acts or omissions relating to non-compliance by a person with any legal obligation imposed on it;

3. Breaches which pose a risk to or are likely to endanger the safety or health of any person;

4. Infringements that cause or are likely to cause damage to the environment.

External reporting channels

In Cyprus, you may report breaches or examples of misconduct that fall within the In-Scope areas, externally using the external reporting channels maintained by the relevant Cypriot competent authorities listed below (note that the list is not exhaustive and may evolve):

- **The FIU (Financial Intelligence Unit**), the national center for receiving, requesting, analyzing and disseminating disclosures of suspicious transactions reports and other relevant information concerning suspected money laundering or financing of terrorism activities. More information on can be found on http://www.law.gov.cy/law/mokas.

- **The Office of the Commissioner for Personal Data Protection (Independent Supervisory Authority for the protection of the individual)**, the independent national public authority responsible for monitoring the implementation of Regulation (EU) 2016/679 (GDPR) and other laws aiming at the protection of individuals with regards to the processing of their personal data. More information can be found on https://www.dataprotection.gov.cy/

- **The Consumer Protection Service, Ministry of Energy, Commerce and Industry**, the public authority authorized to monitor and oversee the enforcement of and compliance with national laws relating to consumer protection in various areas ranging from product safety, unfair trading practices, loans and other credit facilities, legal product warranties, online shopping, package travel and holidays and other. More information can be found on https://consumer.gov.cy/

- **The Commission for the Protection of Competition** the independent competent competition authority of the Republic. It has the authority to implement and enforce legislative provisions prohibiting concerted practices between undertakings and abuse of dominant position. More information can be found on http://www.competition.gov.cy/

- **The Cyprus Independent Authority against Corruption**, the independent authority established pursuant to the law possesses a wide array of powers including the power to investigate acts of corruption either ex officio or following the filing of a complaint, supervise actions within the public, wider public and private sectors, evaluate whether such actions are compatible with determined targets in accordance with internationally recognised best practices and standards, draft reports with opinions, suggestions and proposals for the purpose of compliance with fundamental principles against corruption as well as liaise with non-governmental organisations, professional bodies and associations in connection with the due exercise of its powers. More information is available on the Authority's website: www.iaac.org.cy

- **Treasury of the Republic of Cyprus** is the independent office tasked with overseeing the lawful and responsible management of the public financial operations by, inter alia, securing an effective and transparent public procurement system, fully aligned with the European acquis. For more information visit: www.treasury.gov.cy

- **Customs and Excise Department at the Ministry of Finance** has functions including, inter alia, the control of movement of harmonised goods from other member states into Cyprus and vice versa, the imposition and collection of excise duties and VAT on such goods, the safeguarding of the security of the supply chain of goods and the protection of consumers' health and safety against goods which do not conform to standards. More information can be found on www.mof.gov.cy

- **Office of the Auditor General of the Republic**, is the independent authority tasked with conducting independent, reliable and appropriately documented financial, performance and compliance audit in the public and wider public sector for purposes, inter alia, of the fight against corruption and interference. More information and links for submitting complaints / reports can be found on http://www.audit.gov.cy/

- **Commissioner for Administration and the Protection of Human Rights (Ombudsman)**, the independent incumbent responsible to deal with individual complaints concerning maladministration, misbehaviour and human rights violations by state authorities and officers. The Ombudsman's website has more information and contact details for filing complaints http://www.ombudsman.gov.cy/

Whistleblower Protection

In addition to the safeguards described under section 6.1. of the Whistleblowing Guidelines, if you blow the whistle, your identity and any information from which it could be deduced, may only be disclosed with your express and free consent with exception to those duly authorised to receive or investigate your concern. There are only very limited exceptions to this rule under the Cypriot Whistleblower Act. For example, disclosure without your consent may be necessary in the case of legal proceedings initiated following your report so as to safeguard the reported person's right to a fair trial.

Should the disclosure of your identity or any information from which it could be deduced, become necessary pursuant to specific legislation in the context of investigations by national authorities or judicial proceedings in Cyprus, you will be informed about the disclosure beforehand, unless such information would risk jeopardising the investigations or judicial proceedings concerned.

Furthermore, the Cypriot Whistleblower Act also provides that if you blow the whistle and are subsequently required to participate as a witness in any criminal proceedings relating to your report, you shall be deemed to be a witness in need of assistance, and measures for witness protection may apply to you in accordance with the Cypriot Witness Protection Law.

Archiving of your complaint and handling of personal data

If you blow the whistle, your complaint / concerns, including any recordings, transcripts and minutes of any meetings, will only be kept for as long as strictly necessary and proportionate for the investigation of your complaint / concern and for your protection and the protection of persons mentioned in the report. In particular, the Cypriot Whistleblower Act provides that:

- Personal data collected in the context of receipt of complaints shall be deleted within three (3) months from the date of completion of the investigation procedure.
- In case where your complaint may lead to the initiation of judicial or disciplinary proceedings either against you or against any person mentioned in your complaint, relevant personal data shall be retained for the duration of those proceedings, including any appeal or objection procedure. After one (1) year has elapsed from the completion of such proceedings, the relevant personal data will be deleted.

EMBRACER GROUP

Appendix E – Country Specific Provisions – Czech Republic

This appendix has been issued by the company, Warhorse Studios s.r.o.

If you are based in the Czech Republic and wish to make a report about a concern, these country specific provisions apply to you.

Who these Guidelines apply to locally

In addition to the individuals set out in section 2.2 above, the Whistleblowing Guidelines apply to job candidates and volunteers based in the Czech Republic who wish to raise a concern.

What concerns these Guidelines apply to locally

In addition to the In-Scope areas set out above, if you observe or become aware of wrongdoings (past, present or that is likely to occur) concerning any of the following issues, immediately report it:

1. Violation which qualifies as a criminal offence;

2. Violation which qualifies as an administrative offence punishable by a fine with upper limit of at least CZK 100,000;

3. Violation of the Czech Whistleblowing Act;

4. Violation of the Czech legal regulation in the In-Scope areas.

How to internally report a breach or concern covered by these Guidelines locally

In addition to the information provided in these Guidelines, please note that:

- The report must contain the direct identification of the whistleblower, or information allowing such identification.

- An anonymous report does not trigger the mandatory steps under the Czech Whistleblowing Act.

- However, once the anonymous whistleblower is identified, such whistleblower becomes protected and the report will be properly investigated.

How to blow the whistle

The possibilities of reporting in writing or orally are set out in section 4.1 of the Whistleblowing Guidelines.

Further and as also set out in section 4.1 of the Whistleblowing Guidelines, the following designated person should be contacted:

- Name: Ian Gulam
- Phone: +46 72 857 70 17
- Email: ian.gulam@embracer.com

What to expect when reporting a concern under the Whistleblowing Guidelines

In addition to the information provided in the Whistleblowing Guidelines, please note that:

1. If requested by the whistleblower, the designated person must allow a personal filing of the report within 14 days.

2. The designated person must confirm the receipt of the report in writing, within 7 days. Furthermore, the designated person shall inform the whistleblower of any action taken, the status of the internal investigation as well as the outcome thereof within a reasonable period of time, but no later than 30 days from the confirmation of receipt. In the event of factually or legally complex cases, this period may be extended once or at most twice with each extension lasting up to 30 days. The designated person is obligated to inform the whistleblower in writing of the extended deadline and the reasons for its extension before the deadline expires.

External reporting locally

The external reporting channel is available on this website: https://oznamovatel.justice.cz/.

Archiving of report and handling of personal data

The personal data is processed while the case is ongoing and for a period of 5 years from the date of receipt of the report.

You also have the right to complain about the processing of personal data to your local supervisory authority, which in the Czech Republic is the Office for Personal Data Protection, www.uoou.cz.

Appendix F – Country Specific Provisions – Denmark

Reporting Concerns

These Guidelines apply to reporting such misconducts that fall within the material scope of the Danish Whistleblower Act (Act no. 1436 of 29 June 2021 as amended). It is therefore possible to report:

1. certain breaches of EU law; and

2. serious crimes and other serious situations.

As regards reports on breaches of EU law, reports may be submitted regarding, for example:

- Offences related to rules on public tenders, product safety and compliance and environmental protection. Please see the detailed rules in Article 2 of EU Directive 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law.

Serious crimes and other serious situations are defined as e.g.:

1. Criminal offences, e.g. misuse of funds, theft, fraud, breach of trust, embezzlement, bribery, etc.;

2. Serious or repeated crimes, including e.g. violation of the Danish Road Traffic Act;

3. Gross or repeated violations of significant internal guidelines, e.g. regarding gifts, financial reporting, etc.;

4. Serious personal conflicts in the workplace, e.g. in the form of sexual harassment or other serious harassment.

As a rule, whistleblowing channels cannot be used in relation to dissatisfaction with salary levels, minor misdemeanors such as violations of internal guidelines on smoking and alcohol consumption and less serious personal conflicts and disagreements.

Duty of confidentiality

The whistleblowing team and anyone who may be involved in connection with investigations of the report are subject to a special statutory duty of confidentiality with regard to the information that is or has been subject to processing within the whistleblowing scheme.

Notification of the person to whom the report relates, as well as other persons

If information about you is reported in the whistleblowing scheme, and the report falls within Embracer Group's whistleblower system, you will as a general rule, not receive any information about the processing of your personal data.

If, on the other hand, the report does not fall within Embracer Group's whistleblowing system, you will be informed of the processing of your personal data in accordance with the rules of the Data Protection Regulation and the Danish Data Protection Act.

Protection of the person submitting the report (the whistleblower)

Embracer Group will not tolerate harassment, retaliatory action or any other forms of sanctions against persons who report a matter to the whistleblower scheme in good faith.

False or misleading information must not be submitted deliberately via the whistleblower scheme. Depending on the circumstances, reports submitted in bad faith may have adverse consequences in respect of employment law for the person who submitted the report. Reference is also made to the Danish Whistleblower Act (Act no. 1436 of 29/06/2021 as amended).

External Reporting Channel

If you do not feel comfortable using Embracer Group's whistleblowing service or would prefer to use an external whistleblower scheme for other reasons, you have the option of using the Danish Data Protection Agency's external whistleblower scheme, where written and verbal reports can be submitted. The Danish Data Protection Agency's whistleblower scheme can be accessed via the Danish Data Protection Agency's website.

Data Protection

The processing of personal data in connection with a report received in the whistleblowing scheme will be on the basis of section 22 of the Danish Whistleblower Protection Act, according to which processing of personal data subject to articles 6, 9 and 10 of the General Data Protection Regulation may take place if the processing of the personal data is necessary to investigate a report received in the whistleblowing system established in accordance with the Danish and Irish Whistleblower Protection Act.

If you wish to complain about the processing of personal data, please contact the Danish Data Protection Agency, Carl Jacobsens Vej 35, DK-2500 Valby, Denmark, dt@datatilsynet.dk.

Appendix G – Country Specific Provisions - Finland

Reporting Concerns

These Guidelines apply to reporting such misconducts that fall within the material scope of the Finnish Whistleblowing Act (1171/2022) (Fi. *laki Euroopan unionin ja kansallisen oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta*) (the "**Finnish Act**").

Local scope of protection

Under the Finnish Act, provisions on whistleblower protection apply to employees in the private and public sector, public officials, independent contractors, shareholders, members of the board or supervisory board, or managing director of an entity or foundation, volunteers, and trainees. In addition, the provisions apply to individuals who receive information during pre-employment negotiations or during an employment relationship that has already ended. Further, the Finnish Act also grants protection to whistleblowers within the categories referred to above who have reported or disclosed trade secrets in connection with reporting information on breaches in order to protect the public interest in accordance with the Trade Secret Act and anonymous whistleblowers, who are later identified.

With regard to the In-Scope areas defined under Section 3.1.1 of these Guidelines, the Finnish Act applies to protection of persons reporting breaches, with the precondition that such reported actions or omissions are: 1) punishable by law; 2) punishable by an administrative penalty of a punitive nature; or 3) may seriously undermine the achievement of the objectives of general interest pursued by the legislation (these preconditions do not, however, apply to the reports specified below).

In addition to the In-Scope areas defined under Section 3.1.1 of these Guidelines, the Finnish Act also applies to reports made on breaches of:

1. national legislation regarding granting, use or recovery of grants or state aid;

2. national competition rules;

3. national legislation regarding corporate tax legislation, aiming for unjustified tax benefit; and

4. other EU or national legislation enacted to protect consumers, not mentioned in the directive.

External Reporting Locally

In Finland, internal reporting is allowed through an external channel, as referred to under Section 4.1 of these Guidelines (Alternative 4). However, under the Finnish Act, internal reporting is the primary channel to report, as external reporting is allowed only if:

1. there is no internal reporting channel in place, or a whistleblower has not been provided with an opportunity to report internally;

2. the whistleblower has reasonable grounds to believe that a report made through the internal reporting channel has not been processed and taken under investigation within the applicable timeframe;

3. the whistleblower has reasonable grounds to believe that the breach cannot be effectively resolved internally; or

4. the whistleblower has reasonable grounds to believe that there is a risk of retaliation.

External reports can be submitted to the local competent authority. The Office of the Chancellor of Justice acts as a centralised external reporting channel in Finland (More information can be found here: https://oikeuskansleri.fi/en/about-whistleblower-protection).

EMBRACER GROUP

Appendix H – Country Specific Provisions – France

These guidelines are implemented in France in compliance with applicable legislation and in particular the law No. 2016-1691 of December 9, 2016 on transparency, fight against corruption and the modernization of economic life (known as the "*Sapin II Law*") and the law n° 2022-401 of March 21, 2022 supplemented by Decree no. 2022-1284 of October 3, 2022. Hereinafter together or separately (the "**French Law**").

In-Scope areas

Under French law, reports or discloses must be made without direct financial consideration and in good faith. In addition, the In-Scope area is expanded beyond Breaches of EU Law to include illegal or dangerous acts such as:

1. criminal offenses;

2. misdemeanours;

3. a threat or harm to the general public interest;

4. a violation or an attempt to conceal a violation of an international commitment regularly ratified or approved by France, a unilateral act of an international organization taken on the basis of such commitment, the European Union law, other applicable laws or regulations, including but not limited to theft or fraud.

Information protected by national security ("*secret de la défense nationale*"), medical secrecy ("*secret médical*"), secrecy of judicial decisions, judicial investigations or judicial enquiries ("*secret des délibérations judiciaires, secret de l'enquête ou de l'instruction judiciaires*"), or legal professional secrecy ("*secret professionnel de l'avocat*") cannot be reported under these Guidelines.

The following individuals are encouraged to use the internal reporting process:

1. all current Embracer France employees, former employees where the information was obtained in the course of that relationship, and individuals who have applied for employment with Embracer France, where the information was obtained in the course of the application;

2. shareholders, partners and holders of voting rights in the general meeting of Embracer France;

3. members of the administrative, management or supervisory body ("membres de l'organe d'administration, de direction ou de surveillance");

4. external and occasional consultants;

5. contractors of the entity concerned, their subcontractors or, where the contractor is a legal entity, members of the administrative, management or supervisory bodies of these contractors and subcontractors, as well as members of their staff.

Reported information must :

- have been obtained in the course of the professional activity;
- relate to facts that have occurred or are very likely to occur within the Company.

The individual raising a concern will be asked to provide their name. Exceptionally, it is possible to raise a concern anonymously if the seriousness of the facts have been established and if the factual elements are sufficiently detailed.

When a report or public disclosure has been made anonymously, the individual whose identity is subsequently revealed has the same protections as any individual.

Raising a concern internally

Embracer will ensure that the individuals receiving the reports are able to perform their duties in respect to these guidelines in an impartial manner by providing the following guarantees:

1. the individuals receiving the reports will be free to process reports under the terms of these guidelines without the need for management approval;

2. the individuals receiving the reports will not be subject to retaliation for performing their duties under the terms of these guidelines;

3. the individuals receiving the reports are individuals who, by virtue of their position or status, have the competence, authority and means to carry out their duties;

4. the individuals receiving the reports shall handle all reports only in accordance with applicable legal requirements;

5. the individuals receiving the reports must conduct any investigation in accordance with the adversarial principle and with an impartial ear;

6. the individuals receiving the reports must immediately report any conflict of interest or other situation that may affect his/her impartiality to the management.

Reports made orally (*e.g.*, by voice message to the telephone number or directly to a supervisor) will be recorded as follows:

1. If the report is collected on a recorded telephone line or other recorded voice mail system, with the consent of the individual raising a concern the individual receiving a report will either: (i) record the conversation on a durable and retrievable medium or (ii) transcribe the entire conversation;

2. If the report is collected over an unrecorded telephone line or other unrecorded voice mail system: the individual receiving a report will make an accurate written transcript of the conversation; and

3. If the report is collected during a videoconference or physical meeting, with the consent of the individual raising a concern: the individual receiving a report will either (i) record the conversation on a durable and retrievable medium or (ii) make an accurate written transcript of the conversation.

The individual raising a concern will have the opportunity to verify, rectify and approve the transcript of the conversation or the minutes (as applicable) by signing them.

The recordings, transcripts and minutes shall be kept only as long as it is strictly necessary and proportionate for the processing of the report and for the protection of the individual raising a concern, the persons targeted and the third parties mentioned therein.

Investigation process

If the whistleblowing team decides not to investigate the reported misconduct, the individual raising the concern will be informed of why the report was not considered to not meet the statutory conditions within one (1) month from when the concern was raised.

Regardless of whether the whistleblowing team decides to proceed with the investigation the local management of Embracer France, HR Manager and Legal Representative may be required to intervene in the investigation process with assistance from third parties, subject to confidentiality requirements linked to the report and persons impacted.

Raising a concern externally

Embracer strongly encourages reports to be made internally to ensure that issues can be resolved promptly. However, if individuals decide to report their concerns externally in compliance with the applicable provisions, the competent authorities are set out below:

- the competent authorities listed in annex of the Decree 2022-1284 which can be found here: Competent authorities);
- the Defender of Rights ("*Défenseur des droits*");
- the competent judicial authority;
- an institution, body or agency of the European Union empowered to collect information on violations falling within the scope of the European directive dated 23 October 2019.

The report may only be made public:

1. after having been raised externally (with or without a previous internal report) without any appropriate measures being taken after the expiration of specific time limits as provided by French law;
2. in case of serious and imminent danger, or in case of imminent or obvious danger to the public interest, especially when there is an emergency situation or a risk of irreversible harm; or
3. if reporting the information to Competent Authorities would put the individual raising the concern at risk of retaliation or would prevent the content of the disclosure from being remedied effectively.

EMBRACER GROUP

Appendix I – Country Specific Provisions – Germany

These country specific provisions (the "**Country Section**") supplement the Embracer Group Whistleblowing Guidelines (the "**Guidelines**") and are applicable at

- **PLAION** (Deep Silver Fishlabs GmbH, Plaion Media GmbH, and Plaion Pictures GmbH);
- **THQ Nordic** (Black Forest Games GmbH);
- **Asmodee** (ADC Black Fire Entertainment GmbH, Asmodee GmbH)

(together "**Embracer Germany**").

For a report to be in scope of application as outlined in this Country Section below, a Reporter has to report a potential breach to the Local Reporting Channel. Only in case of reporting to the Local Reporting Channel in accordance with this Country Section, the German Whistleblower Protection Act ("**GWPA**") shall apply.

In the event of a conflict between the Guidelines and this Country Section, this Country Section shall prevail.

Personal Scope of the Country Section

This Country Section applies to employees at Embracer Germany, persons employed at Embracer Germany for their vocational training, persons who, due to their economic dependence, are to be regarded as equivalent to employees ("*Arbeitnehmerähnliche Personen*") and Contingent Workers (as defined in the European Union Whistleblower Policy) at Embracer Germany, but also to persons who have acquired information about Breaches (as defined below) in the context of a working or professional relationship with Embracer Germany, such as business partners or suppliers. This Country Section also applies to those who report a Breach of which they became aware during a recruitment process or pre-contractual negotiations with Embracer Germany (collectively "**Reporters**").

Material Scope of this Country Section

This Country Section covers the reporting of the following potential breaches in relation to the activities of Embracer Germany (each a "**Report**"):

- Violations that are subject to criminal liability (*Verstöße, die strafbewehrt sind*)
- Violations which are subject to administrative fines (*Verstöße, die bußgeldbewehrt sind*) provided the violated regulation serves to protect life, limb or health or to protect the rights of employees or their representative bodies
- Offences of federal and state legislation as well as directly applicable legal acts of the European Union and the European Atomic Energy Community related to : (i) public procurement; (ii) financial services, products and markets, and/or prevention of money laundering and/or terrorist financing; (iii) product safety and/or compliance; (iv) transportation safety; (v) environmental protection; (vi) radiation protection and/or nuclear safety; (vii) food and/or food safety, animal health and animal welfare; (viii) public health; (ix) consumer protection; (x) protection of privacy and/or personal data and/or the security of networks and/or network and information systems;
- Offences of tax law applicable to corporations and commercial partnerships;

- Offences in the form of agreements aimed at improperly obtaining a tax advantage contrary to the objective or purpose of the tax law applicable to corporations and commercial partnerships;
- Offences affecting the financial interests of the European Union, such as breaches of the relevant anti-fraud or anti-corruption legislation;
- Offences relating to the internal market, in particular breaches of the rules on competition and/or State aid

(together, the "**Breaches**")

How to report a potential Breach covered by this Country Section internally

In Germany, Reporters may raise a concern by using the Alternatives 1 to 3 mentioned in Section 4.1 of the Whistleblowing Guidelines. However, this means the concern will be heard and potentially investigated using group resources and this Country Section as well as the GWPA will not apply.

If Reporters wish to have the concern heard and investigated locally, please report to the German local reporting channels available on https://report.whistleb.com/embracer (also see Section 4.2 of the Guidelines) ("**Local Reporting Channels**")**.**

There are three different local reporting channels depending to which entity you belong to:

- **PLAION Germany Local Reporting Channel** (for the entities Deep Silver Fishlabs GmbH, Plaion Media GmbH, and Plaion Pictures GmbH)
- **Black Forest Games GmbH Local Reporting Channel** (for the entity Black Forest Games GmbH)
- **Asmodee Germany Local Reporting Channel** (for the entities ADC Black Fire Entertainment GmbH, and Asmodee GmbH).

Reports may be made through anonymous or confidential messaging, and, at the request of a Reporter and according to their choice, during a videoconference or a physical meeting.

Investigation process

Reporters can report potential Breaches via the Local Reporting Channel identified in Section 3 of this Country Section.

Reports received through the Local Reporting Channels are processed by appointed individuals that are responsible for the respective local reporting channel.

Confidentiality

The whistleblower's identity as well as the identity of the person who is subject of the Report, any third party mentioned in the Report and any information received in connection with the Report form which the identity may be directly or indirectly deduced will be processed in a confidential manner in accordance with applicable law**.**

Record Keeping

The documentation has to be deleted three years after the investigation procedure is completed. The documentation may be retained longer in order to comply with

requirements under the German Legislation or other legislation as long as it is necessary and proportionate.

Protection against retaliation

Retaliation against those making Reports in good faith and persons who facilitate or otherwise assist in the making of the Report or the investigation process will not be tolerated; in particular, they will not be at risk of losing their job or suffering any form of sanctions or personal disadvantages as a result of the Report.

External Reporting Channels

Embracer strongly encourages reports to be made internally for concerns to be resolved as soon as possible. However, should employees decide to report their concerns externally in compliance with applicable provisions the competent authorities are set out in the Whistleblower Protection Act (*Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden*). In particular, the local external reporting channels can be found here.

The reporting person may also make a Report to institutions, bodies, offices or agencies of the European Union, such as:

- European Commission
- European Anti-Fraud Office (OLAF)
- European Maritime Safety Agency (EMSA)
- European Union Aviation Safety Agency (EASA)
- European Securities and Markets Authority (ESMA)
- European Medicines Agency (EMA).

EMBRACER GROUP

Appendix J – Country Specific Provisions – Italy

Reporting Concerns

These Guidelines apply to reporting misconducts that fall within the material scope of the Italian Whistleblowing Decree (Legislative Decree no. 24/2023) (the "**Decree**"), these are the following:

1. administrative, accounting, civil or criminal violations which are not deemed as relevant under points (iii), (iv), (v) and (vi) below;

2. any relevant misconduct according to Legislative Decree no. 231/01, or violations of any relevant provisions provided under the company management model in accordance with the above Legislative Decree no. 231/01, if any;

3. any relevant misconducts in violation of the European Union or local regulations, even if not regulated by any Italian law provisions, related to: (i) public procurement; (ii) financial services, products and markets, and prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transportation safety; (v) environmental protection; (vi) radiation protection and nuclear safety; (vii) food and feed safety, animal health and animal welfare; (viii) public health; (ix) consumer protection; (x) protection of privacy and personal data, and the security of networks and network and information systems; (x) any other relevant violations according to administrative, criminal, civil regulations;

4. any relevant misconduct listed under Article 325 of the Treaty on the Functioning of the European Union;

5. any relevant acts or omissions relating to the local market, as referred to in Article 26(2) of the Treaty on Functioning of the European Union, including violations of the European Union competition and State aid rules, as well as infringements relating to the local market related to acts in breach of corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law;

6. any relevant acts of omissions in breach of the object or purpose of the provisions of any European Union acts in the areas indicated in points (iii), (iv) and (v) above.

The following are expressly excluded from the scope of application of the Whistleblowing Guidelines:

1. facts, information, documents, regardless of their form or medium, the disclosure of which is prohibited because they are covered by national security, medical secrecy, secrecy of judicial deliberations, judicial investigations or judicial enquiries or legal professional secrets;

2. interpersonal conflicts are also excluded.

The persons, in the context of an employment or professional relationship, who can report internally through the internal local reporting channel referred under **section 4** above, subject to the conditions set out in the Whistleblowing Guidelines ("**Reporters**"), are the following:

1. employees, former employees, persons who are self-employed;

2. shareholders and members of the managing, governing or supervisory body of the concerned company, including non-executive members;

3. volunteers;

4. paid or unpaid trainees;

5. any person working under the supervision and direction of contractors, subcontractors or suppliers;

6. individuals who receive information during the recruiting process or pre-employment negotiations.

The protections provided by the Decree apply to the Reporters and also extend to:

1. the legal representatives of employees in the exercise of their functions of advising and supporting the Reporter;

2. individuals who, within the organisation in which the Reporter works, assist the Reporter in the reporting process;

3. individuals who are related to the Reporter and who may suffer reprisals, such as co-workers or relatives of the Reporter; and

4. individuals for whom the Reporter works or with whom he/she has any other type of relationship in an employment context or in which he/she has a significant shareholding.

Procedural aspects

We encourage the use of the **local report channels referred to under Section 4.2 of the Whistleblowing Guidelines** and available on https://report.whistleb.com/embracer, when the report involves concerns relevant at an Italian level.

The Reporter may also request a meeting in person to report the concerns. In such case, the face-to face meetings will be carried out though online meetings by using a dedicate application (e.g. Microsoft Teams, Zoom, etc.).

Verbal communications, including those made through face-to-face meetings shall be documented in one of the following ways, subject to the Reporter's consent:

1. by means of a recording of the conversation; or

2. by a complete and accurate transcription of the conversation (the Reporter can verify, rectify and agree to the transcription of the conversation by signing it).

The transcripts and minutes may only be kept for the time strictly necessary and proportionate to the processing of the report and to the protection of the Reporter, the persons they refer to and the third parties they mention, as well as to preserve the Company's defence right, taking into account the time required for any further investigations.

However:

1. retention of the reports may be extended to take account of any complementary investigation;

2. data relating to the reports may be kept for longer than necessary provided that data is anonymized and the concerned individuals are neither identified nor identifiable.

In any case, Reporters may be sanctioned if the competent Italian Authority should find that they reported false information when submitting the report. In such case, disciplinary sanctions could be applied.

Reports that contain information obtained unlawfully (e.g., information contained in stolen documents) or that, reasonably, appear to be unlawfully obtained will not be accepted nor can be used by Embracer to take corrective measures.

If the local Operative Group considers that the report would be managed more effectively by involving another Embracer Group's legal entity or the Embracer Group alone, it will inform the Reporter that the report will be funnelled either to:

1. the Embracer Group's Channel; or

2. the local Operative Group of the other entity concerned. The Italian Operative Group remains responsible and accountable for maintaining confidentiality, giving feedback, and addressing the reported concern. In such case, the sharing of the Report will be subject to the consent expressed by the Reporter.

If a Reporter submits a concern anonymously to the local Operative Group, the latter should label the report as "anonymous" and carry out the relevant investigation ensuring the confidentiality of the Reporter's (as well as other involved individuals') identity is always protected. Even if the Reporter has not given their name, the duty of confidentiality extends to any other information for which the identity of the Reporter may be directly or indirectly deduced.

Protections for the Reporters

The identity of the Reporter or any information from which this identity can be retrieved may be disclosed only with the Reporter's consent, unless such disclosure is required by a public authority (e.g., by a Public Prosecutor). The Reporter's identity may be disclosed to Embracer's internal and external professionals (e.g., lawyers, forensic teams, etc.) involved in any internal investigation. These individuals are subject to a strict duty of confidentiality and cannot share this information, unless specifically authorized by the Reporter. If the Reporter's identity must be disclosed to a public authority, the Reporter will be informed with due notice, unless this may impair the investigation or legal proceedings or breach any relevant public regulation.

The identity of the person who is the subject of the report as well as the identity of any third party mentioned in the report must also be processed in a confidential manner, in accordance with the Whistleblowing Guidelines. The information collected as a result of the report can be disclosed to third parties only if necessary for the processing of the report and for the implementation of disciplinary or corrective measures.

Any acts (direct or indirect) of retaliation against the Reporter are prohibited, including but not limited to:

1. dismissal, suspension or equivalent measures;
2. demotion or lack of career advancement;
3. change of duties, place of work, salary reduction, change of working hours;
4. suspension from training or any restriction to access training;
5. negative referrals or admonitions;
6. disciplinary measures or (even monetary) sanctions;
7. coercion, intimidation, harassment or ostracism;
8. discrimination or in any case less favourable treatments;
9. failure to confirm fixed-term employees where the employee had a legitimate expectation to said confirmation;
10. failure to renew or early terminate fixed-term employment contracts;
11. damages (also reputational), particularly on social media, economic prejudices (e.g., loss of chances);
12. insertion on black lists;
13. early termination or annulment of service or goods supply contracts;
14. annulment of licenses and authorizations;
15. requests of medical or psychiatric visits.

All material relating to the Reporter and the report will be treated in such a way not to alter the report and ensure that identity of the Reporter and of any other individual concerned by the report is not disclosed, unless this is necessary to follow up on the reports and adopt all the relevant corrective measures.

The individuals that are subject of or mentioned in the report must be informed of the existence of the report within a reasonable period of time. This information may be delayed if it is likely that this disclosure may seriously jeopardize the investigations (e.g., where there is a risk that evidence might be destroyed). When disclosing the existence of the report, the identity of the Reporter or other third parties cannot be disclosed in any case.

It is expressly forbidden to disclose information about complaints or possible internal investigations. Likewise, the confidentiality of the documentation generated during the investigation is guaranteed.

Non-compliance with confidentiality obligations and non-observance of the prohibition of retaliation constitutes very serious misconduct.

External Reporting Channel

Embracer strongly encourages reports to be made internally for concerns to be resolved effectively.

However, in Italy, if a Reporter decides to report their concerns externally in compliance with applicable local provisions, the competent authority is the National Anti-Corruption Authority ("**ANAC**").

External reports to ANAC can be made on: https://whistleblowing.anticorruzione.it/#/

Data protection

The local Operative Group and the individuals entrusted with the investigation activities may process personal data of the Reporters, the persons who are the subject of the reports and any other person involved in the report or any subsequent investigation.

The data controllers of personal data is **Milestone S.r.l.**, with registered office at Via Olona no. 2, Milan, Italy.

The purpose of processing personal data is managing the Italian reporting channel and investigating the reports in accordance with the legal provisions regarding the implementation of a whistleblowing system pursuant to the Decree.

Personal data will only be accessed by the relevant local Operative Groups.

However, without prejudice to the strict above-mentioned confidentiality obligations, access to personal data may be granted upon the individual's consent, as a mere example, to HR supervisors, managers, local Compliance Officers, company functions or any other individual involved in the investigations so they can take all the necessary disciplinary measures or take legal action to solve the reported issue.

Reporters, persons subject of the report or other affected individuals may exercise their data privacy rights as described in the data controller's privacy notices. However, in the event that the persons who are the subject of the reports exercise their right to object, it shall be presumed that there are compelling legitimate grounds for processing his or her personal data, unless there is evidence to the contrary.

Personal data relating to out-of-scope reports, special categories of personal data (except where necessary due to the nature of the report), untruthful information, and personal data that is unnecessary for the investigation should not be collected or if collected because necessary - in first instance - will be destroyed without delay.

Appendix K – Country Specific Provisions – The Netherlands

Reporting Concerns

These Whistleblowing Guidelines apply to reporting such misconducts that fall within the material scope of the Dutch Whistleblower Protection Act (in Dutch: "*Wet bescherming klokkenluiders*"), (the "**Dutch Act**"), which are the following:

1. a breach or risk of a breach of Union law, or

2. an act or omission with regard to which the public interest is at stake in connection with:
   - a breach or risk of a breach of a statutory regulation or of internal rules that impose a specific obligation and have been established by Embracer Group on the basis of a statutory regulation; or
   - a risk to public health, public safety or the environment, or an improper act or omission that jeopardizes the proper functioning of Embracer Group. A public interest is in any event at stake if the act or omission affects more than just personal interests and is either part of a pattern or structural in nature, or is serious or broad in scope.

Non-retaliation

Retaliation against those making reports, whether direct or indirect, will not be tolerated. This protection against retaliation provided by the Dutch Act, also extends to:

1. facilitators who advise a reporting person in the reporting process in a work-related context and whose advice is confidential;

2. a third party who is connected with a reporting person and who could suffer a detriment at the hands of the reporting person's employer or a person or organisation with which the reporting person is otherwise connected in a work-related context;

3. a legal entity that the reporting person owns, works for or is otherwise connected with in a work-related context; and

4. the designated independent officer or officers to whom a suspected wrongdoing can be reported and the independent officers who will follow up on the report.

External Reporting Channels

Embracer Group strongly encourages reports to be made internally so that any concerns can be resolved. However, should employees decide to report their concerns externally, the competent authorities are set out below:

- Authority for Consumers and Markets (*Autoriteit Consument en Markt*) (https://www.acm.nl)

- Authority for Financial Markets (*Autoriteit Financiële Markten*) (www.afm.nl)

- Data Protection Authority (*Autoriteit persoonsgegevens*) (www.autoriteitpersoonsgegevens.nl)
- De Nederlandsche Bank N.V. (www.dnb.nl)
- House for Whistleblowers (*Huis voor Klokkenluiders*) (www.huisvoorklokkenluiders.nl)
- Health and Youth Care Inspectorate (*Inspectie gezondheidszorg en jeugd*) (www.igj.nl)
- Dutch Healthcare Authority (*Nederlandse Zorgautoriteit*) (www.nza.nl)
- Authority for Nuclear Safety and Radiation Protection (*Autoriteit Nucleaire Veiligheid en Stralingsbescherming*) (www.autoriteitnvs.nl)
- Other authorities appointed by the minister or statute

Information on how to report can be found on the respective authority's website. You may also seek advice on a confidential basis from the Advice Department of the Dutch Whistleblowers Authority (in Dutch: "*Huis voor Klokkenluiders*") before reporting any breaches (advies@huisvoorklokkenluiders.nl).

Appendix L – Country Specific Provisions – Romania

Who the Whistleblowing Guidelines apply to locally?

The Whistleblowing Guidelines apply to the following categories of people who wish to report a workplace-related concern (the "**Whistleblowers**"):

1. Current or former employees of Embracer Group in Romania,

2. Third-party contractors, sub-contractors, suppliers, consultants, or agency workers, both current or former, who performed work or provided services for or to Embracer Group,

3. Shareholders and persons belonging to the administrative, management or supervisory body of Embracer Group, including the non-executive members of the board of directors,

4. Volunteers, as well as paid or unpaid trainees,

5. Any persons working under the supervision and direction of contractors, subcontractors and suppliers who performed work or provided services for or to Embracer Group,

6. Job candidates in relation to a recruitment process at Embracer Group, who obtained information in relation to their concern during the recruitment process or other pre-contractual negotiations,

7. Potential service providers to Embracer Group, such as manufacturers, suppliers, contractors, or consultants, who obtained information in relation to their concern during the pre-contractual negotiations,

8. Persons who anonymously report or publicly disclose information regarding violations of the law.

Reporting Concerns

The Whistleblowing Guidelines apply to reporting such misconducts that fall within the material scope of the Romanian Whistleblowing Law (Law 361/2022) (*Legea nr. 361/2022 privind protecţia avertizorilor în interes public*), which are the following:

1. Misconducts in breach of the European Union law falling within the scope of the Whistleblowing Directive as set out in Section 3.1 in the Whistleblowing Guidelines (the "Scope") above;

2. Breaches falling within the scope of the Romanian laws and Union acts set out in the Annex 2 to the Romanian Whistleblowing Law that concern the following areas:
   - Public procurement;
   - Financial services, products and markets, and prevention of money laundering and terrorist financing;
   - Product safety and compliance;
   - Transport safety;

- Protection of the environment;
- Radiation protection and nuclear safety;
- Food and feed safety, animal health and welfare;
- Public health;
- Consumer protection;
- Protection of privacy and personal data, and security of network and information systems.

3. Breaches related to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union (TFEU), including breaches of the European Union rules on competition and State aid, as well as breaches related to the internal market in terms of acts that violate the rules on corporate taxation or mechanisms whose purpose is to obtain a fiscal advantage that contravenes the object or purpose of the law applicable to corporate taxation, which represents disciplinary misconducts, contraventions or crimes, or which are contrary to the object or purpose of the law.

What a whistleblowing message should contain

According to the Romanian Whistleblowing Law, a whistleblowing message should include, at least, the following:

1. the name and the contact details of the whistleblower,

2. the workplace-related context in which the information was obtained,

3. the person concerned, if known,

4. the description of the fact likely to constitute a violation of the law within the company (i.e. Embracer Group) and, as appropriate,

5. the evidence in support of the report,

6. the date and signature if the case.

If the whistleblowing message does not contain the above mentioned elements, other than the whistleblower's identification data, the whistleblower may be asked by the whistleblowing team to provide additional information to your message within fifteen (15) days. If the whistleblower fails to provide the requested information within the foregoing timeframe, the respective report will be closed without further due.

Anonymous reporting

Anonymous reports will be analysed to the extent they contain indications of the alleged breach of the law.

You may be asked by the whistleblowing team to provide additional information to the anonymous whistleblowing message within fifteen (15) days. If the whistleblower fails to provide the requested information within the foregoing timeframe, the anonymous whistleblowing report will be closed without further actions taken in relation to such report.

Record keeping

The whistleblowing reports are stored for a period of five (5) years, as provided under the Romanian Whistleblowing Law.

External Reporting Channels

As per the Romanian Whistleblowing Law, the whistleblower can submit a whistleblowing message/report to external reporting channels.

The National Agency for Integrity is the authority with general competencies in relation to external whistleblowing reporting.

Further information on how you can report a concern externally according to the Whistleblowing Guidelines can be found on the website of the National Agency for Integrity, respectively on: Informații generale – Avertizori în interes public (integritate.eu)

Other aspects

If the whistleblower is subject to a disciplinary proceeding due to a fake, misleading or defamatory whistleblowing report (whether through internal or external reporting channels, or public disclosure), the relevant disciplinary committee or similar body within local Embracer Group entity shall, based on the prior request of the whistleblower, invite the media, a representative of the European Union or professional association, or a representative of the employees. Such invitation shall be made on the local Embracer Group entity's website at least three (3) business days prior to the disciplinary hearing.

EMBRACER GROUP

Appendix M – Country Specific Provisions – Spain

This Country-specific Addendum for Spain (the "**Spanish Addendum**") describes the specific requirements applying to the Local Reporting Channel implemented by the local ASMODEE subsidiary Asmodee Editions Iberica SLU in Spain ("**Embracer Spain**")

This Spanish Addendum supplements the Group Whistleblowing Guidelines (the "Guidelines") and prevails over the Guidelines in case of conflict.

Material Scope of the Local Reporting Channel

In addition to the In-scope areas listed under Section 3.1 of the Guidelines, breaches in the following areas may be reported through Embracer Spain's Local Reporting Channel:

- Acts or omissions that may constitute "serious" or "very serious" administrative infringements or criminal offences, including all serious or very serious administrative infringements or criminal offences that involve economic loss for the Public Treasury and for Social Security.

If the individuals within the Personal Scope (as defined in the Guidelines and this addendum) do not report any breach that she/he is aware of, this could result in disciplinary actions.

Personal Scope of the Local Reporting Channel

These Guidelines apply to Embracer Spain employees but reports from persons who have acquired information about the breaches outlined above in the context of a working or professional relationship with Embracer Spain or any other legal entity within Embracer may also be accepted. The categories of persons who may report by virtue of their working or professional relationship, in addition to employees of Embracer Spain, include:

- independent contractors;
- any person working under the supervision and direction of contractors;
- sub-contractors service providers or suppliers;
- members of the board;
- members of management;
- shareholders;
- auditing or supervisory corporate bodies;
- non-executives;
- volunteers and trainees;
- former employees or;
- candidates.

Local Reporting Manager

The impartial person who is competent for receiving and following-up on the reports, which will maintain communication with the Whistleblower and, where necessary, ask for further information from and provide feedback to that Whistleblower is: Jose Manuel Rey Breval jm.rey@asmodee.com.

In the event that Jose Manuel Rey Breval is absent from work/ conflicted, the report can be submitted to Sabina Sala (s.sala@asmodee.com) or via the Asmodee Operative Group

Reporting channel (with Céline Bucki, c.bucki@asmodee.com and Elisabeth Elkaim, e.elkaim@asmodee.com as receivers of reports) or via the Embracer central group channel.

Reporting concerns locally

The Local Reporting Channel is accessible via the reporting platform at https://report.whistleb.com/embracer which allows written or oral online reporting.

The Whistleblower may also submit a report by means of a face-to-face meeting with the Local Reporting Manager (or the person delegated by him/her) within a maximum of seven (7) days.

If the report is done verbally or through a face-to-face meeting, at the Whistleblower's choice: (i) the conversation shall be recorded on a durable and retrievable medium or (ii) an accurate written record of the conversation shall be made. The Whistleblower shall have the opportunity to verify, rectify and approve the transcript of the conversation or the minutes (as applicable) by signing them (electronically, if applicable).

When a report is received, the Local Reporting Manager will provide written acknowledgment of receipt of the same within seven (7) days, provided that the confidentiality of the communication is not compromised.

Upon receipt of the report, the Local Reporting Manager shall make a preliminary assessment as to whether the facts reported are within the material scope of these Guidelines (and therefore considered "**In-Scope Breaches**"), as well as the consistency and the plausibility of the facts reported. The Local Reporting Manager may request additional information from the Whistleblower if deemed necessary.

In order to carry out the aforementioned preliminary analysis of the report and the adoption of the decision to admit or reject it for processing, the Local Reporting Manager may ask the corresponding internal department (depending on the specific subject matter of the complaint submitted) for support in the analysis and decision making process. This support may be requested from persons within Embracer Spain and/or persons belonging to other Group companies. Likewise, the Local Reporting Manager may request the support of external professionals at any time. All of this while guaranteeing the confidentiality of the information and providing specific personal data strictly on a need-to-know basis.

The Local Reporting Manager, shall lead the investigation of the report, establishing the necessary internal and external resources for the same (that will normally include the appointment of an investigator and an investigation team), as well as the persons who must have access to the report and to the information obtained from the report and from the internal investigation process (including personal data such as the identity of the Whistleblower).

The Local Reporting Manager may ask the corresponding internal department (depending on the specific subject matter of the complaint submitted) for support in the investigation process. This support may be requested to other Embracer Group entities. Likewise, the Local Reporting Manager may request the support of external professionals at any time. This will be done while ensuring the confidentiality of the information and providing specific personal data strictly on a need-to-know basis.

Once the investigation is concluded, the corresponding actions will be adopted according to Embracer Guidelines and procedures and applicable local law.

The Local Reporting Manager may maintain communication with the Whistleblower and, if deemed necessary, request additional information from the Whistleblower on the submitted report.

In any event, the Local Reporting Manager will contact the Whistleblower in writing within three (3) months of initial receipt of the report or, if no response is received, within three months of the expiration of a period of seven calendar days following the report, to respond to the investigative actions, providing summary information on the steps planned or taken to follow up on the complaint and address the alleged breach reported, all subject to Embracer Spain's other obligations (e. g. confidentiality and personal data protection obligations). In cases of particular complexity requiring an extension of the three (3) month maximum period, this may be extended by up to a maximum of three (3) additional months.

The confidentiality of the information contained in the report and obtained during the investigation process shall be protected according to the applicable laws.

Please note that if a Report is not received through the reporting channels mentioned in these Guidelines but through other unofficial channels, the employee receiving such Report must immediately communicate the same to the Local Reporting Manager within a maximum of 48 hours and immediately delete the Report received. The person who has received the Report must keep the Report strictly confidential. Failure to comply with these reporting and confidentiality obligations may lead to disciplinary action.

Safeguards

Protection against retaliation

Individuals benefit from the protection provided by applicable Spanish statutory provisions. In addition to the Whistleblower, the following individuals are protected against retaliation:

1. The legal representatives of employees in the exercise of their functions of advising and supporting the Whistleblower;

2. Individuals who, within the organization in which the Whistleblower works, assist the Whistleblower in the process;

3. Individuals who are related to the Whistleblower and who may suffer reprisals, such as co-workers or relatives of the Whistleblower;

4. Individuals for whom the Whistleblower works or with whom they have any other type of relationship in an employment context or in which they have a significant shareholding.

In particular, the Whistleblower and these individuals are protected against any form of (threats and attempts of) retaliation (including termination, demotion, suspension, loss of benefits, threats, harassment or discrimination).

When a Report or public disclosure has been made anonymously, the individual whose identity is subsequently revealed has the same protections as any Whistleblower.

Rights and obligations of the affected person

The affected person has the right to be informed of the facts attributed to him/her as soon as possible and to be heard at any time. Such communication shall take place in a time and manner which is deemed appropriate to ensure the proper conduct of the investigation.

The investigation shall be conducted with full respect for the honour, the presumption of innocence and the right of defence of the affected person, preserving his or her identity and guaranteeing the confidentiality of the facts and the data of the internal investigation.

The affected person must maintain confidentiality in relation to the existence of the complaint and investigation and may not threaten or coerce any person who is collaborating with the investigation. Failure to comply with these obligations may result in disciplinary sanctions.

Data protection and processing

Embracer Spain will be the data controller of the personal data processed for the purpose of managing the Local Reporting Channel and investigating the reports, according to its obligation to comply with legal provisions regarding the implementation of a whistleblowing system pursuant to the Spanish Legislation.

The Local Reporting Manager (and his/her team) may process personal data of the Whistleblowers and the affected persons. In particular, the following categories of personal data may be collected and processed as part of the receipt and subsequent investigation of reports:

1. Identity, functions and contact details of the Whistleblowers;
2. Identity, functions and contact details of the persons who are subjects of the report;
3. Identity, functions and contact details of persons involved in the collection or processing of the report;
4. Facts reported;
5. Elements collected within the framework of the verification of the reported facts;
6. Investigation reports; and
7. Follow-up to the report.

The purposes of processing this data are (i) to assess the reports received through the Local Reporting Channel, (ii) to carry out the necessary internal investigations (iii) to record the operation and effectiveness of the Local Reporting Channel and to (iv) adopt the necessary measures to address the reports received.

The lawful basis for the processing of data received as a result of a report or in the framework of a subsequent internal investigation is Article 6(1)(c) of the General Data

Protection Regulation (EU) 2016/679. In other words, the processing is necessary for compliance with the legal obligation to have an internal whistleblowing channel.

Personal data will only be accessed by the Local Reporting Manager (and his/her team) although they may allow access to HR for taking disciplinary measures, the Legal Team for taking legal action, to the data protection officer, to any third party where necessary for taking corrective measures, and to data processors that may assist with the management or reports and/or investigations. The Local Reporting Manager may also involve other internal professionals for the purpose of conducting an internal investigation. These are subject to a strict duty of confidentiality

The processing of personal data managed through the Local Reporting Channel for Spain includes the following obligations:

1. No personal data shall be collected or processed if it is not manifestly relevant to the processing of a specific Report. If collected by accident, the data shall be deleted without undue delay.

2. Any personal data contained in Reports which relate to conduct that does not fall within the material scope of the Embracer Whistleblowing Guidelines or this Addendum will be deleted. If the information received contains personal data falling within the special categories of data, it shall be deleted immediately, without undue delay.

3. Any report that is proven to be untrue shall be immediately deleted, unless such untruthfulness may constitute a criminal offence, in which case the report shall be kept for the time necessary for the duration of the legal proceedings.

4. All reports which have not been followed up and which are intended to be kept shall be anonymized, without identifying any individual who is a party to the report or file;

5. Individuals within the personal scope of application of this Addendum shall be informed of the processing of personal data that takes place within the framework of the Local Reporting Channel. In addition, when personal data is obtained directly from the individuals, they shall be provided with the legally required information on the processing of such data and shall be informed that their identity shall be kept confidential in all cases.

6. If the report is made through a physical meeting and is to be recorded, the Whistleblower shall be warned of such recording and shall be informed of the processing of his or her data in accordance with the provisions of the Data Protection Regulations. In addition, such recording shall be aligned with other applicable internal policies.

7. The affected person shall in no case be informed of the identity of the Whistleblower or of the person who has made the public disclosure, even if he/she exercises his/her right of access to his/her personal data.

8. The data processed may be kept in the Local Reporting Channel only for the time necessary to decide whether or not to initiate an investigation. In any case, it shall be deleted after three (3) months have elapsed from the receipt of the Report without any investigation being initiated, unless the purpose of the storage is to leave evidence of the operation from the Local Reporting Channel.

9. Once the three (3) month period has elapsed, the data may continue to be processed outside the Local Reporting Channel, for the development of the investigation of the reported facts, or when necessary for the execution of civil, criminal, labor, administrative, disciplinary or any other type of action. Once the investigation has been completed, the data shall be kept in the register-book for a maximum period of ten (10) years, except when it should be retained for a longer time in order to safeguard Embracer Spain's right of defence.

Personal data subjects may exercise, in accordance with the Data Protection Regulations, their rights of access, rectification, deletion, opposition, limitation of processing and portability of their data, where applicable according to the applicable regulations, by sending an e-mail to the address comunicacion@asmodee.com, personal data subjects may exercise their rights in accordance with the relevant privacy notice, available at https://asmodee.es/politica-de-privacidad/.In addition, they also have the possibility of lodging a report with the relevant supervisory authority. In the case of Spain, this is the Spanish Data Protection Agency (www.aepd.es).

However, the exercise of such rights does not apply when it concerns a report relating to the prevention of money laundering and terrorist financing, in which case the provisions of article 32 of Law 10/2010, of 28 April, shall apply. In addition, in the event that the target person exercises the right to object, it shall be presumed that there are compelling legitimate reasons that legitimize the processing of their personal data, unless there is evidence to the contrary.

External Reporting Channels

Embracer Spain strongly encourages reports to be made internally through any of the reporting channels available for concerns to be resolved appropriately and quickly. However, should the Whistleblowers decide to report their concerns externally in compliance with applicable provisions, they can report to the Independent Authority for the Protection of Informants or the corresponding independent authorities for the protection of informants created at regional level.

Appendix N – Country Specific Provisions - Sweden

Reporting Concerns

These Guidelines apply to reporting such misconducts that fall within the material scope of the Swedish Whistleblowing Act (2021:890) (Sw. *lag om skydd för personer som rapporterar om missförhållanden*) (the "**Act**"), which are the following:

1. Misconducts in breach of the European Union law falling within the scope of the Whistleblowing Directive as set out in section 3.1 in the Whistleblowing Guidelines (the "Scope") above;

2. Misconducts in breach of Swedish law that implement or supplement European Union law falling within the Scope;

3. Other misconducts that are such that it is in public interest that they are disclosed

Misconducts that are of public interest means that the public must have a legitimate interest in being informed about the misconduct in order to, for example, either remedy the misconduct or take measures to protect themselves. **Circumstances relating to your own work or employment relationship are often not considered to be in the public interest.**

Examples of what may constitute misconduct of the public interest and therefore may be considered as reporting issues, may include criminal offences, irregularities and violations or other actions in breach of European Union or Swedish law within a work-related context, such as the breaches described in section 3.1 in the Whistleblowing Guidelines. However, the protection for reprisals under Chapter 3 in the Act may be applicable even if the conduct does not constitute a direct breach of European Union or Swedish law. Deviation from Embracer Group's adopted Code of Conduct or other policies, which gives the business a competitive advantage (such as a commitment not to apply slave-like working conditions) may also constitute a misconduct of public interest.

Freedom to Communicate Information

Please note that under the Swedish Freedom of Press Act (Sw. *tryckfrihetsförordning*) and the Swedish Fundamental Law on Freedom of Expression (Sw. *yttrandefrihetsgrundlag*) everyone is free to communicate information on any subject whatsoever for the purpose of publication in programs or technical recordings (freedom to communicate information, Sw. *meddelarfrihet*) as well as right to procure information on any subject whatsoever in order to communicate or publish it (freedom to procure information, Sw. *anskaffarfrihet*).

External Reporting Channels

In Sweden, you may also report misconducts using the external reporting lines maintained by the competent authorities listed below (note that the list is not exhaustive and may evolve). Information on how to report can be found on the respective authority's website.

Swedish Work Environment Authority (Sw. Arbetsmiljöverket)

The Swedish Work Environment Authority is the supervisory authority for employers' handling of whistleblowing. The Swedish Work Environment Authority also has an external reporting channel for misconduct covered by EU legislation and by the Swedish Work Environment Authority's supervision, i.e. product safety and product compliance, that you have become aware of in a work-related context.

Information on how to report can be found on the Swedish Work Environment Authority's website https://www.av.se/.

The Swedish National Board of Housing, Building and Planning (Sw. Boverket)

In Boverket's external channel, you can report misconduct in a work-related context that has to do with product safety and product compliance. It must also be an instance of misconduct that falls within the Boverket's supervisory responsibility.

Information on how to report is available on Boverket's website https://www.boverket.se/. Here you will also find a direct link to the platform.

National Electrical Safety Board (Sw. Elsäkerhetsverket)

You can report serious irregularities such as illegal manufacture, import or distribution of products covered by the LVD, EMC, ATEX, Radio Equipment or Toys Directives, the Gas Appliances Regulation and the General Product Safety Directive.

Information on how to report is available on the National Electrical Safety Board's website https://www.elsakerhetsverket.se/.

Swedish Economic Crime Authority (Sw. Ekobrottsmyndigheten)

The whistleblowing function of the Swedish Economic Crime Authority deals exclusively with misconduct affecting the EU's financial interests. These may include:

- fraud
- subsidy abuse
- certain customs offences
- certain VAT offences
- acts in breach of conditions for EU aid
- false certification in certain cases, corruption, double funding, etc.

Information on how to report can be found on the website of the Swedish Economic Crime Authority: https://www.ekobrottsmyndigheten.se/.

The Swedish Estate Agents Inspectorate (Sw. Fastighetsmäklarinspektionen, FMI)

If you are connected to the broker industry, you can contact the FMI if you become aware that someone within a broker company is violating money laundering rules.

Information on how to report can be found on the FMI website https://fmi.se/.

The Financial Supervisory Authority (Sw. Finansinspektionen, FI)

FI receives reports from persons who, in a work-related context, wish to provide FI with information about misconduct that is in the public interest. A report must relate to a concrete suspicion that a company or a private individual has violated a regulatory framework that falls under FI's supervisory responsibility.

Information on how to report can be found on FI's website https://www.finansinspektionen.se/.

Public Health Agency (Sw. Folkhälsomyndigheten)
The Public Health Agency of Sweden receives reports of tobacco-related abuses that fall under its supervision.

Information on how to report can be found on the Public Health Agency's website https://www.folkhalsomyndigheten.se/.

Swedish Agency for Marine and Water Management (Sw. Havs- och vattenmyndigheten)
The Swedish Agency for Marine and Water Management receives notifications of irregularities detected in the area of responsibility of the Agency and concerning supervision or regulatory guidance in the field of environmental protection and economic matters such as public procurement.

Information on how to report can be found on the Agency for Marine and Water Management's website https://www.havochvatten.se/.

Swedish Authority for Privacy Protection (Sw. Integritetsskyddsmyndigheten, IMY)
You can report to IMY if you have information that the person you work or have worked for, or are applying to work for, is not complying with the General Data Protection Regulation (GDPR) or additional rules, such as the Data Protection Act.

Information on how to report can be found on the IMY website https://www.imy.se/.

Inspectorate of Strategic Products (Sw. Inspektionen för strategiska produkter, ISP)
The ISP, as a competent authority, receives reports from persons who, in a work-related context, wish to provide information on violations falling within the ISP's remit under the Act.

Information on how to report can be found om the ISP website http://www.isp.se/.

The Health and Social Care Inspectorate (Sw. Inspektionen för Vård och Omsorg, IVO)
The area of responsibility in the field of public health which is covered by the authority's supervisory responsibility is blood, tissue and transplant activities.
IVO is also responsible for malpractice in the area of privacy and personal data protection and network and information system (NIS) security, which falls under the Authority's supervisory responsibility.

Information on how to report can be found on Ivo's website: https://www.ivo.se/.

The Swedish Chemicals Agency (Sw. Kemikalieinspektionen, Kemi)
You can report whistleblowing to Kemikalieinspektionen to report violations of certain chemicals legislation for which Kemi is the competent authority. An example
of such misconduct is when a company imports toys containing unauthorized chemical products into Sweden.

Information on how to report can be found on Kemi's website https://www.kemi.se/.

The Swedish Consumer Agency (Sw. Konsumentverket)
You can report complaints concerning product safety, public health and consumer protection that fall within the scope of the Consumer Agency's supervision, in accordance with legislation common to the EU Member States.

Information on how to report can be found on the Consumer Agency's website https://www.konsumentverket.se/.

Swedish Competition Authority (Sw. Konkurrensverket)
If you discover a violation in the areas of competition
and public procurement in a work-related context, you can report it to the Swedish Competition Authority in accordance with the Act. The violation may, for example, concern incorrect direct procurement, unauthorised price cooperation or contractual conditions that harm competition.

Information on how to report can be found on the Competition Authority's website https://www.konkurrensverket.se/.

Swedish Food Agency (Sw. Livsmedelsverket)
You can report irregularities concerning product safety/product compliance, environment radiation protection and nuclear safety, food, animal health and safety and data privacy that fall under the Swedish Food Agency's supervisory responsibility.

Information on how to report can be found on the Food Agency's website https://www.livsmedelsverket.se/.

Swedish Medical Products Agency (Sw. Läkemedelsverket), MPA
If you discover irregularities in an activity that concerns the MPA's supervisory responsibility, you can report it to the MPA.

Information on how to report can be found on the MPA's website https://www.lakemedelsverket.se/sv.

County Administrative Boards (Sw. Länsstyrelserna)
The County Administrative Boards receive and handle reports of non-compliance in the areas of product safety/product compliance, environmental protection, prevention of money laundering and financing of terrorism. Each county has its own channel.

Information on how to report can be found on the County Administrative Board's website https://www.lansstyrelsen.se/.

Swedish Civil Contingencies Agency (Sw. Myndigheten för samhällsskydd och beredskap, MSB)
The Swedish Civil Contingencies Agency receives, follows up and provides feedback on reports of nonconformities in the area of product safety and product compliance that fall under the Swedish Civil Contingencies Agency's market surveillance responsibilities.

Information on how to report can be found on the Swedish Civil Contingencies Agency website https://www.msb.se/.

The Swedish Environmental Protection Agency (Sw. Naturvårdsverket)
You can notify PTS of serious irregularities or breaches of regulations in the areas of product safety and conformity, protection of privacy and personal data,
or security of network and information systems.

Information on how to report can be found on the PTS website https://www.naturvardsverket.se/.

The Swedish Post and Telecom Authority (Sw. Post- och telestyrelsen, PTS)
You can notify PTS of serious irregularities or breaches of regulations in the areas of product safety and conformity, protection of privacy and personal data,
or security of network and information systems.

Information on how to report can be found on the PTS website https://www.pts.se/.

Government Offices of Sweden (Sw. Regeringskansliet)
Abuses relating to state aid can be reported to the Government Offices.

Information on how to report can be found on the Government's website https://www.regeringen.se/.

Swedish Inspectorate of Auditors (Sw. Revisorsinspektionen)
You can report misconduct to the Inspectorate of Auditors if what someone does or what someone has failed to do is contrary to the provisions applicable to authorized and approved auditors and to registered audit firms.

Information on how to report can be found on the Inspectorate's website https://www.revisorsinspektionen.se/.

The Swedish Tax Agency (Sw. Skatteverket)
The Tax Agency's external whistleblowing function only concerns certain abuses in the field of taxation covered by EU legislation, namely abuses in the financial interests of the EU in the field of taxation and internal market abuses in the field of corporate tax.
For example, a company may have carried out or will carry out transactions aimed at circumventing or exploiting tax legislation in order to obtain a tax advantage. For example, it may involve transactions of a tax avoidance nature. In most cases, tax avoidance involves practices whereby a taxpayer carries out one or more transactions primarily for the purpose of obtaining or avoiding a tax effect, such as seeking a deduction for a false loss.

Information on how to report can be found on the Swedish Tax Agency's website https://www.skatteverket.se/privat.4.76a43be412206334b89800052864.html.

The Swedish Forest Agency (Sw. Skogsstyrelsen)
You can notify the Swedish Forest Agency of irregularities that fall under the Agency's supervisory responsibility. Information on how to report can be found on the Swedish Forest Agency's website https://www.skogsstyrelsen.se/.

The Gaming Inspectorate (Sw. Spelinspektionen)
The Swedish Gaming Inspectorate is responsible for receiving whistleblowing reports concerning irregularities in the area of prevention of money laundering and financing of terrorism within the authority's supervisory area, i.e. gaming companies licensed in Sweden.

Information on how to report can be found on the Spelinspektionen's website https://www.spelinspektionen.se/.

The Swedish Energy Agency (Sw. Statens energimyndighet)
The Swedish Energy Agency works to prevent corruption and irregularities. In case of suspicion of serious irregularities within the Swedish Energy Agency. More information on how to report can be found here: https://report.whistleb.com/sv/Energimyndigheten.

Sweden's national accreditation body (Sw. Styrelsen för ackreditering och teknisk kontroll, SWEDAC)
Swedac's area of competence is misconduct in the field of product safety and product conformity that falls under Swedac's supervisory responsibility and that contravenes the directives to which the Whistleblowing Directive applies.

More information on how to report can be found on Swedac's website https://www.swedac.se/.

The Swedish Board of Agriculture
For those who want to safely report misconduct in the area of environmental protection and which are covered by the authority's supervisory responsibility.

Information on how to report can be found on the website of the Board of Agriculture: https://jordbruksverket.se/.

Swedish Radiation Safety Authority (Sw. Strålsäkerhetsmyndigheten)

For those who want to safely report misconduct in a work-related context in the field of radiation protection and nuclear safety that falls under the regulatory responsibility of the Agency.

Information on how to report can be found on the website of the Radiation Safety Authority: https://www.stralsakerhetsmyndigheten.se/.

Swedish Transport Agency (Sw. Transportstyrelsen)

If, in a work-related context, for example as an employee, you have such information that you have reasonable grounds to believe that your operator is in breach of EU law, you can, in certain cases, make a notification to the Swedish Transport Agency.

Information on how to report can be found on the Swedish Transport Agency's website https://www.transportstyrelsen.se/sv/vagtrafik/.