Merlin Entertainments – Global Whistleblowing policy

1 Accessibility Statement

Merlin Entertainments Group (the **Group** or **Merlin**) recognises the importance of providing materials in a way that is accessible to all audiences. If you need this document in large print or another accessible format, please contact your HR department.

2 About this policy

2.1 Merlin is committed to the highest possible standards of openness, integrity and accountability and encourages any individual who has genuine concerns about an alleged breach in the organisation (e.g., unethical behaviour, forms of malpractice, illegal acts, failure to comply with regulatory requirements, accounting irregularities, or violations of Group policy) to raise those concerns at an early stage through Merlin's internal reporting channel.

2.2 A Breach is any event, incident, situation, act, or omission believed to violate Group (or a Group company's) policy or procedure or an applicable law or regulation, related to the areas of concern listed in article 4 of this policy (**Breach** or **Breaches**).

2.3 You are encouraged to share any concerns or information regarding Breaches, including reasonable suspicions about actual or potential Breaches, whether occurring within Merlin or being committed by an entity or an individual acting on Merlin's behalf, as well as any attempts or suspected attempts to conceal a Breach.

2.4 Merlin strives to foster a workplace conducive to open communication regarding the Group's business practices. We are committed to ensuring any individual who reports an actual or potential Breach through the reporting channels set out in this policy is protected from unlawful retaliation and discrimination if they make a report with reasonable grounds to believe the information in the report is true. Merlin takes all reports of actual or potential Breaches seriously and is committed to ensuring that reported Breaches are addressed discretely and effectively within Merlin to determine the appropriate course of action in accordance with applicable Group policy and all applicable laws, including but not limited to the stipulations of the European Directive of 23 October 2019 on the protection of persons who report breaches of Union law (2019/1937).

2.5 In furtherance of these commitments, this policy:

(a) gives guidance on the receipt, retention, and treatment of verbal or written reports of actual or suspected Breaches received by Merlin;

(b) gives guidance on how to report information regarding an actual or suspected Breach in a confidential and, where applicable, anonymous manner; and

(c) makes clear Merlin's intention to discipline or terminate the employment of any person determined to have engaged in retaliatory or discriminatory behaviour.

2.6 This policy is separate to Merlin's normal grievance procedure. If you have a complaint relating to your own personal circumstances or concerns about matters such as harassment and bullying, you should refer to any local grievance policies on these issues, or speak to your local Human Resources

Department for advice. If you are unsure as to which policy applies to your circumstances, you should seek guidance, in confidence, from your local Human Resources Department.

3 Scope

This policy applies to the following individuals who acquire information on a reportable Breach in a work-related context:

3.1 employees or workers with permanent or limited-term contracts;

3.2 contractors;

3.3 sub-contractors;

3.4 volunteers;

3.5 paid or unpaid trainees;

3.6 agency workers where the worker is supplied by a third person to Merlin; and

3.7 self-employed individuals.

4 Concerns covered by the policy

4.1 This policy is designed to cover the reporting of an actual or suspected Breach including but not limited to Breaches involving the following areas:

(a) public procurement;

(b) financial services, products and markets;

(c) prevention of money laundering;

(d) prevention of terrorist financing;

(e) product safety and compliance;

(f) transport safety;

(g) protection of the environment;

(h) radiation protection and nuclear safety;

(i) food and feed safety;

(j) animal health and welfare;

(k) public health;

(l) consumer protection;

(m) protection of privacy and personal data;

(n) security of network and information systems;

(o) Breaches affecting the financial interests of the EU;

(p) Breaches relating to the EU internal market including Breaches of:

(i) competition and State aid rules;

(ii) rules on corporate tax including any tax arrangements;

(q) any misconduct such as violations of local laws or regulations that could potentially give rise to criminal or regulatory liability for Merlin or its employees, including but not limited to:

(i) allegations of anti-corruption and sanctions;

(ii) account irregularities;

(iii) fraud;

(iv) conflict of interest;

(v) misappropriation of assets.

4.2 You are encouraged to report any Breach which you reasonably believe is unlawful and is causing you concern.

4.3 Your report can relate to any Breach anywhere in the world; it is not restricted to matters purely arising in the country where you work.

4.4 Whilst this policy is intended to be global in nature, there are some additional provisions that apply to specific jurisdictions, which are set out in the Appendices to this Policy.

5 Protection against retaliation

5.1 Merlin appreciates that the decision to raise a concern can be a difficult one to make, not least because there may be a fear of reprisal from those who may be involved the Breach (e.g. those who may have committed the Breach, etc). Merlin will not tolerate retaliation against any person who raises a concern through the reporting channels provided in this policy where they have reasonable grounds to believe that the information in the report is true at the time of reporting, even if it transpires that there is no basis for concluding that any Breach has occurred, or is likely to occur. In addition, Merlin prohibits discrimination on the grounds of gender, gender reassignment, marital or civil partnership status, race, colour, nationality, ethnic origin, national origin, disability, age, sexual orientation, religion or belief, or any other prohibited grounds, when addressing concerns that have been raised.

5.2 The protections against retaliation and discrimination also apply, where relevant, to:

(a) facilitators;

(b) third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context; such as colleagues or relatives of the reporting persons; and

(c) legal entities that the reporting person owns, works for or are otherwise connected with in a work-related context.

5.3 Merlin will take appropriate steps to protect all impacted individuals, including taking necessary action, which may include but is not limited to disciplinary action or dismissal, against anyone who is found to be pursuing any form of retaliation or discrimination, or has threatened to do so.

6 False allegations

Just as Merlin will seek to protect those who raise concerns where they have reasonable grounds to believe that the information in the report is true at the time of reporting, it will also protect those who

are accused of a Breach in a report which is false. Merlin will take necessary action against any individual who knowingly reports false information, which may include but is not limited to disciplinary action or dismissal.

7 Raising a concern

7.1 General principles

(a) Merlin encourages individuals to raise suspected Breaches when it is just a concern, as long as they have reasonable grounds to believe that the information in the report is true, rather than waiting for proof or investigating the matter themselves. Acting sooner rather than later can avoid any further potential damage. Reports will be treated with confidentiality.

(b) Merlin encourages individuals to ask questions and discuss concerns with their supervisor, who can often be an excellent resource. However, Merlin recognizes that you may not always feel comfortable raising concerns with a supervisor and, as such, you can report any concern via the internal reporting channels, as detailed below.

(c) Reports may be made on an anonymous basis, but individuals are encouraged to submit their name with their report. Concerns expressed anonymously are less powerful and tend to be more difficult to address effectively, but will nonetheless be considered and dealt with by the Group to the fullest extent possible.

7.2 Methods of reporting

(a) You can make a report of a Breach under this policy in one of two ways:

(i) by reporting it internally; or

(ii) by using Merlin's whistleblowing hotline or online portal.

7.3 Internal reporting

(a) In the first instance, you should report any concern to your line manager, either in person, in writing or both. If you believe your line manager to be involved in the suspected wrongdoing, or do not otherwise wish to contact your line manager, then you should contact your local Human Resources Department, Head of Department or General Manager / Divisional Director.

(b) If you are not comfortable reporting your concern at a local level, you may alternatively raise the concern at a Group level to the Group HR Director, Chief Corporate Officer, Acting Chief Financial Controller, Group Health, Safety & Security Director or Group Reward Director, whose contact details are as follows:

Please contact your local People Team for contact details.

7.4 Whistleblowing hotline / portal

(a) If you do not wish to report your concern internally, you are encouraged to use Merlin's whistleblowing hotline or portal, both of which are operated externally by Safecall. Safecall is a completely independent company that operates a confidential reporting service for many global businesses and it is available 24 hours a day and is staffed by highly skilled professional call handlers.

(b) You can make calls to the hotline free of charge from anywhere in the world. Where English is not your first language, a translator will be provided for you within a few minutes.

(c) SafeCall will take the details of your concern and raise them to a Merlin whistleblowing contact. Merlin will then investigate the concern and feedback will be given to you via SafeCall.

(d) Through using the whistleblowing hotline it is possible for your identity to be kept confidential from Merlin. However, as mentioned above, reporting a concern anonymously makes it more difficult to investigate and address effectively.

(e) A full list of the international Freephone numbers can be found online at https://www.safecall.co.uk/file-a-report/telephone-numbers. The numbers for countries in which Merlin operates are also listed in the appendix to this policy

(f) Where you do not wish to raise a concern internally, you are encouraged to use the whistleblowing hotline telephone numbers as a preferred method of raising a concern; as the hotline enables you to speak to a real person directly in local language and ensures that concerns can be raised as a matter of urgency where the issue is time critical.

(g) However, as an alternative to calling the whistleblowing hotline, you may also raise a whistleblowing concern online via the SafeCall secure online portal. The portal is secure as all information is encrypted for security reasons. To raise a concern online please visit the following URL: www.safecall.co.uk/report

(h) You can file an online report in your preferred language and can select your preferred language from the welcome page before submitting a report.

(i) However, you should be aware that it may take a little longer for concerns raised via the online portal to be processed as opposed to contacting the telephone hotline where calls will receive an instant response from SafeCall.

7.5 Procedure for reporting

(a) All reports of actual or suspected Breaches must be factual and contain as much information as possible. All reported information, including about the identity of the reporter, is treated as confidential subject to applicable legal and regulatory requirements.

(b) If you choose to make an internal report, this will normally be acknowledged within 48 hours of receipt. Where possible a call or meeting will be arranged in order to further investigate the concern. You may be accompanied at any meeting by a colleague or a representative from a union or another employee representative body. However, any companion must respect the confidentiality of the disclosure and any subsequent investigation.

(c) If you choose to make an oral report via Merlin's whistleblowing hotline, the Safecall call handler will take notes and may ask you questions based on the account you give. Safecall will produce a written report for Merlin. All Safecall reports, or internal reporting under this policy will normally be escalated to Merlin's Group Reward Director and its Internal Audit & Risk Management Director initially, who will then allocate the report to the most appropriate person in the business to address it.

(d) Upon receipt of a concern (whether received directly or via Safecall) the Group will carry out an assessment to determine the scope of investigation required. You may be asked to provide further information to assist with investigations. If you have used the whistleblowing hotline or online portal, all communication, including any additional questions to be asked, will be conducted through SafeCall. Every reporter is given their own login details to the portal which can be accessed from https://report.safecall.co.uk and clicking "sign-in". Any further requests for information and updates will be posted on the relevant report within your portal.

(e) The appointed Merlin investigator will aim to keep you informed of the progress of the investigation and its likely timescale, either directly or via the SafeCall portal.

(f) The appointed Merlin investigator will be responsible for:

(i) maintaining communication with you including asking for further information on the report, where necessary;

(ii) ensuring your report is diligently followed up/investigated to assess the accuracy of the allegations made in the report;

(iii) ensuring a decision is made on any action required to address the breach reported or deciding to close the procedure;

(iv) providing feedback to you on your report including information on action envisaged or taken as follow-up to the report and the grounds for such follow-up. Feedback will be provided within a reasonable timeframe which will not exceed three months from acknowledgement of receipt of your report.

7.6 Operating principles for investigating complaints

(a) An investigation to establish all relevant facts will be conducted as sensitively and speedily as possible.

(b) Investigations will normally be carried out by an independent investigator who has had no previous involvement in the matter.

(c) In some instances it might be necessary to refer the matter to an external authority for further investigation, such as the Police.

(d) At the end of the investigation, the investigator will analyse all the evidence and make findings of fact, based upon the balance of probabilities, as to whether a Breach has occurred or is likely to occur.

(e) Whilst the Group will endeavour to provide an outcome to all complaints, you should be aware that, sometimes the need for confidentiality may prevent the Group from giving you specific details of the investigation or any disciplinary action taken as a result.

(f) Any information provided to you about an investigation or its outcome should be treated as confidential.

7.7 Appeals

(a) Whilst the Group cannot always guarantee the outcome employees are seeking, it will try to deal with concerns fairly and in an appropriate way.

(b) If you are not happy with the way in which your concern has been handled, you can raise it with one of the other key contacts listed in this policy (or escalate it via the SafeCall response portal).

7.8 Keeping and managing records

(a) When an individual makes an internal report, Merlin will process any personal data collected in compliance with applicable laws and regulations and in accordance with its Data Protection Policy and Employee Data Privacy Notice (where applicable). Data collected from the point at which an individual makes the report is held securely and accessed by, and disclosed to, only authorised individuals and only for the purposes of dealing with the report.

(b) Personal data collected by Merlin as a consequence of a report under this policy will be incorporated to a database controlled by the Group, for the purposes of processing the report and conducting any investigation required. Merlin may also need to share personal data with other companies/subsidiaries within the Group, external investigative agencies, legal counsel and/or local authorities. Such third parties may be based in territories outside the EU, like the

United States of America, which do not offer an equivalent level of protection on data privacy as in EU. Nevertheless, if data transfers outside the EU are needed, Merlin will take appropriate measures to protect the data according to local regulations.

(c) Personal data which are not relevant for the handling of a specific report will not be collected or, if accidentally collected, will be deleted without undue delay.

(d) Merlin recognises that it is important, and in everyone's interests, to keep written records during the concern raising process. Records will be stored for no longer than is necessary and in a way that is proportionate to comply with Merlin's data privacy obligations and record-keeping obligations. Records that will be retained and treated as confidential, include:

(i) the nature of the concern raised;

(ii) a copy of any written notification setting out the nature of the concern;

(iii) key documents/evidence;

(iv) the investigation workpapers;

(v) the investigator's report;

(vi) any written response by Merlin, including any action taken and the reasons for action taken; and

(vii) minutes of meetings.

(e) Where an individual requests a meeting for reporting purposes, Merlin will ensure, subject to the consent of the individual, that complete and accurate records are kept of the meeting which will be either:

(i) by making a recording of the conversation; or

(ii) through accurate minutes of the meeting prepared by the staff member responsible for handling the report. The reporting individual will be offered the opportunity to check, rectify and agree the minutes of the meeting by signing them.

7.9 Duty to cooperate and preserve relevant evidence

From time to time, you may be asked to provide or preserve documents related to an investigation or may receive a request to participate in an investigative interview. All individuals subject to this policy are obliged to cooperate with Group investigations by timeously providing truthful accounts and relevant documents in response to interviews, questions and information requests. The destruction of documents or other evidence related to an investigation is prohibited. Any individual who fails to cooperate, or otherwise obstructs, impedes or improperly influences an investigation, or attempts to do so, will be subject to disciplinary action, or even termination of their employment, in accordance with Merlin's applicable policies.

7.10 External reporting channel

This policy provides individuals with the opportunity and protection necessary to raise concerns internally through a central reporting procedure (either internally or via an independent third party) and Merlin believes that the processes laid out herein are the most effective processes for dealing with reports of a Breach in a manner that serves the best interests of both Merlin and any individual making a report. However, if you feel that you cannot raise your concerns in this way and reasonably believe the information you wish to report is true, you may consider reporting the matter to a competent external authority. See Country Specific Rules if applicable.

8 Confidentiality

Merlin's internal reporting processes are secure and confidential which means that:

8.1 no unauthorised person is allowed access to information held within it;

8.2 the identity of an individual who makes a report, together with any other information from which their identity may be directly or indirectly deduced, will be kept confidential and protected and will not be disclosed, without the individual's consent, to anyone beyond authorised individuals within Merlin or their designees who are competent to receive or follow-up on a report;

8.3 by way of an exception, and subject to appropriate safeguards under the applicable European Union and national rules, the identity of a reporting person and any other information from which their identity might be deduced, may be disclosed where this is necessary in the context of an investigation by any national authority or in the context of judicial proceedings;

8.4 where an individual is referred to in a report as a person to whom a Breach is attributed or with whom someone who committed a Breach is associated, Merlin will ensure that the individual's identity is kept confidential and protected for so long as investigations triggered by the report are ongoing and will ensure that the individual is treated fairly including being given the presumption of innocence and a right to be heard.

9 Contractual status

This policy does not form part of any employee's contract with Merlin, however, Merlin expects that its principles and procedures should be followed by all individuals within its scope. Merlin reserves the right to change the content of this policy, as necessary, from time-to-time.

10 No waiver of rights

The rights of individuals to report concerns under this policy cannot be waived or limited by any agreement, policy, form or condition of employment and Merlin will never require any such waiver or limitation of rights by any individual.

Whistleblowing Hotline International Freephone Telephone Numbers

A full list of international freephone numbers is available online from https://www.safecall.co.uk/file-a-report/telephone-numbers

Country	Freephone Number to call	Alternative Number
Australia	1800312928	
Austria	0080072332255	
Belgium	00 800 72332255	
Canada	1 877 599 8073	
China	10800 744 0605 (China Unicom/Netcom)	10800 440 0682 (China Telecom)
China (Shared Cost)	4008 833 405	
Denmark	00 800 72332255	
Finland	990 800 7233 2255 (Telia Sonera)	999 800 7233 2255 (Elisa)
France	00 800 72332255	
Germany	00 800 72332255	
Hong Kong	3077 5524	
Iceland	00 800 7233 2255	
India	000 800 4401 256	
Ireland	1 800 812 740	
Italy	00 800 7233 2255	
Japan	0120 921 067	
Korea	001 800 7233 2255 (Korea Telecom	002 800 7233 2255 (DACOM)
Malaysia	1800 220 054	
Netherlands	00 800 7233 2255	
New Zealand	00 800 7233 2255	
Portugal	00 800 7233 2255	
Singapore	800 448 1773	
Spain	00 800 7233 2255	
Thailand	001 800 7233 2255	
Turkey	00 800 4488 20729	
United Arab Emirates	8000 441 3376	
United Kingdom	0800 915 1571	
United States	1 866 901 3295	

Country specific rules for Italy

1 Purpose of this Appendix

1.1 This Appendix to the Merlin Entertainments – Global Whistleblowing policy ("**Policy**") provides for special requirements and deviations applying for Italy based on the Italian Legislative Decree No. 24/2023 ("**Italian Whistleblowing Decree**"). In the following, the individual sections of the Policy are listed and – where necessary – supplemented by corresponding additions and amendments for Italy.

1.2 In the event of a contradiction between the provisions in the Policy and this Appendix, the latter shall prevail. In the event of a contradiction between the Policy and/or this Appendix and applicable Italian laws and regulations (in particular the provisions set out in the Italian Whistleblowing Decree), the Italian laws and regulations shall prevail, as well as for any mandatory provision not expressly covered by the Policy and/or this Appendix.

2 Scope (Section 3 of the Policy)

2.1 This Appendix applies to the following individuals who acquire information on a reportable Breach in the work-related context (collectively, "**Reporting Persons**"):

i. employees or workers with permanent or limited-term contracts;

ii. contractors;

iii. sub-contractors;

iv. volunteers;

v. paid or unpaid trainees;

vi. agency workers;

vii. advisors and self-employed individuals;

viii. shareholders and persons entrusted with functions of administration, management, control, supervisory or representation, even when such functions are exercised on a de facto basis.

2.2 The Reporting Persons may report:

ix. when the legal relationship has not yet started, if the information on Breaches was acquired during the recruitment process or another pre-contractual negotiation stage;

x. during the probationary period;

xi. during the entire employment relationship;

xii. after the termination of the legal relationship, if the information on Breaches was acquired during the course of the latter.

3 Concerns covered by the Policy (Section 4 of the Policy)

3.1 For '**Report**' is intended the oral or written communication of information concerning actual or potential Breaches, including reasonable suspicions, which occurred or are very likely to occur in the work-related context.

3.2 Breaches that may be reported pursuant to the Italian Whistleblowing Decree are:

I. unlawful conduct relevant under the Italian Legislative Decree No. 231/2001 ("**Decree 231**") (*i.e.*, constituting one or more offences under the catalogue of offences entailing corporate liability), or constituting a violation of the Organization, Management and Control Model adopted under Decree 231 ("**Model 231**") (*i.e.*, rules of conduct and/or principles of control), which are not included in the following;

II. breaches of EU or national acts (including those implementing EU law) relating to the following areas: (a) public procurement; (b) financial services, products and markets and prevention of money laundering and terrorist financing; (c) product safety and compliance; (d) transport safety; (e) protection of the environment; (f) radiation protection and nuclear safety; (g) food and feed safety and animal health and welfare; (h) public health; (i) consumer protection; (l) protection of privacy and personal data, security of network and information systems;

III. acts or omissions constituting fraud or other illegal activity detrimental to EU financial interests as set out in Article 325 of the TFEU and detailed in EU relevant secondary legislation;

IV. acts or omissions affecting EU internal market compromising the free movement of goods, persons, services and capital, including breaches of EU antitrust provisions, State aids and corporate tax rules, as well as any mechanism aimed at obtaining a tax advantage which frustrates the object or purpose of the applicable corporate tax law;

V. acts or conduct which, in any event, frustrate the object or purpose of EU acts in the areas indicated above.

3.3 Reports may also concern:

i. conduct aimed at concealing the above Breaches;

ii. illegal activities not yet committed that the Reporting Person reasonably believes may occur based on concrete, precise and concordant elements;

iii. well-founded and concrete suspicions inherent in the information indicated above.

3.4 The following do not constitute reportable information for the purposes of the present Appendix:

i. mere rumors and 'hearsay';

ii. disputes, claims or requests related to an interest of a personal nature of the Reporting Person that pertain exclusively to his/her individual working relationships, or that are inherent to his/her working relationships with hierarchically superior figures;

iii. communications of information on breaches where already mandatorily regulated by EU or national acts (also implementing EU law) as indicated in Part II of the Annex to the Directive and the Italian Whistleblowing Decree (in the areas of services, products and financial markets and prevention of money laundering and financing of terrorism, environmental protection and transport safety) – in relation to which the discipline and related specific reporting procedures, where existing, are applied;

iv. communication of information on national security breaches, as well as breaches of procurement rules involving defence or national security aspects, unless the aforementioned aspects are covered by EU secondary legislation;

v. communication of information whose disclosure is prohibited by EU or national law related to classified information, legal and medical professional privilege, secrecy of investigations and deliberations of judicial bodies (or other provisions of criminal procedure).

4 Raising a concern – Internal reporting (Section 7.3 of the Policy)

4.1 Without prejudice to the possibility of reporting centrally to Merlin Entertainments using the channels described in the Policy above, in Italy, any Reports can be made at a local level through the Italian internal reporting channel operated by a **Committee** designated to carry out this function, which also includes a component of the Supervisory Board (Organismo di Vigilanza - O.d.V.).

(a) The Reporting Person may make a report orally or in writing:

(i) to make an oral report by requesting a meeting in person with the **Committee**, after scheduling an appointment, by sending an e-mail to the following address segnalazioni.whistleblowing@gardaland.it.

Where the Reporting Person chooses to make a report in person, the **Committee** shall either record the conversation or draft a complete and accurate conversation transcript. The Reporting Person shall have the opportunity to check, correct and ensure the accuracy of the conversation written transcript.

(ii) to make a written report by ordinary mail, bearing the Reporting Person's identifying data and marked "*Private and Confidential/Whistleblowing Report*" to the postal address Gardaland S.r.l., Via Derna, 4 - 37014 Castelnuovo Del Garda (VR) Italia.

Having received a Report via ordinary mail, the **Committee** will ensure the confidential protocoling of the Report. In particular, the same will be placed by the **Committee** in two sealed envelopes: the first one bearing the Reporting Person's identifying data together with a photocopy of the ID; the second one containing the Report, so as to separate the Reporting Person's identifying data from the Report itself. Both envelopes shall, afterwards, be placed in a third sealed envelope bearing the wording "*Strictly Private and Confidential/Whistleblowing Report*" on the outside.

(b) The Reporting Person may also make a report through SafeCall – which allows for anonymous reporting as well – available at the following link www.safecall.co.uk/report, following the instructions therein, indicating the country [Italy] and the legal entity to which the Report is addressed [Gardaland].

(c) all reports of actual or suspected Breaches must be factual and contain as much information as possible. All reported information, including about the identity of the reporter, is treated as confidential subject to applicable legal and regulatory requirements;

(d) The **Committee** will be responsible for:

(i) acknowledging receipt within seven (7) days of the Report;

(ii) maintaining communication with the Reporting Person including asking for further information on the Report, where necessary;

(iii) ensuring the Report is diligently followed up/investigated to assess the accuracy of the allegations made in it, and informing the Supervisory Body ("Organismo di Vigilanza" – "OdV") about the Breaches indicated in point I of paragraph 3.2 of the Appendix (*i.e.* related to unlawful conduct relevant under Decree 231 or to a violation of the Organization, Management and Control Model adopted under Decree 231);

(iv) ensuring a decision is made on any action required to address the Breach reported or deciding to close the procedure;

(v) providing feedback to the Reporting Person on the Report including information on action envisaged or taken as follow-up to the Report and the grounds for such follow-up. Feedback will be provided within a reasonable timeframe which will not exceed three (3) months from acknowledgement of receipt of the Report. Where investigations take longer than three (3) months, the Reporting Person will be provided with information on the *status* of the investigation process, whose conclusion will nevertheless be communicated to the Reporting Person processing personal data

collected throughout the entire whistleblowing procedure in compliance with the GDPR and national Data Protection applicable legislation, for the purposes of processing the report and conducting any investigation required. Specifically, personal data may be shared with other companies within the Group, external investigative agencies, legal counsels and/or local authorities to properly investigate and provide feedback to the reporter. These third parties may be based in territories outside the EU, which do not offer an equivalent level of Data Protection as in EU. Nevertheless, if data transfers outside the EU are needed, appropriate measures to protect the data will be granted in accordance with local laws.
Personal data which are not relevant for the handling of a specific report will not be collected or, if accidentally collected, will be deleted without undue delay.

4.2 Persons in the work-related context other than the **Committee** receive, by mistake, a Report relevant under this Appendix shall:

i. guarantee the integrity, confidentiality and privacy of all the information referred to in the Report received in compliance with the provisions of paragraph 8;

ii. forward the Report – accompanied by any supporting documentation received - without withholding a copy, immediately (and in any case within seven (7) days of receipt) and exclusively to the **Committee**, in all cases with the obligation to refrain from taking any independent initiative for analysis and/or investigation;

iii. where possible, simultaneously informing the Reporting Person that the Report has been forwarded to the person in charge of managing it in accordance with this Appendix, and also informing him/her of the advisability of making the Report through the channels specifically made available.

5 Raising a concern – External reporting channel (Section 7.10 of the Policy)

5.1 As indicated in section 7.10 of the Policy, if the Reporting Person feels that they cannot raise their concerns via the internal (local) reporting channel and reasonably believe the information they wish to report is true, they may consider reporting the matter to a competent external authority. With regard to Italy, it is also guaranteed an external reporting channel managed by Italian Anti-Corruption Authority (**ANAC**).

5.2 In this respect, the Reporting Person could report externally to ANAC:

(a) if the internal reporting channel, despite being mandatory, is not active or, even if active, does not comply with the provisions set forth by the Italian Whistleblowing Decree as it is not suitable to guarantee the obligations of confidentiality of involved persons;

(b) if the Reporting Person filed a Report locally, through the internal reporting channels, but the Report was not followed up;

(c) if the Reporting Person has well-founded reasons to assume that Report through the internal reporting channel will not be effectively followed up, or that the same Report might lead to the risk of retaliation;

(d) if the Reporting Person has well-founded reasons to believe that the Breach may constitute an imminent or manifest danger to the public interest.

5.3 To submit a report via ANAC reporting channel, please click on the link below:

https://whistleblowing.anticorruzione.it/#/

6 Protection against retaliation (Section 5 of the Policy)

6.1 In accordance with the provisions set out in Section 5 of the above Policy, any behaviour, act or omission, even if only attempted or threatened, carried out as a consequence of the Report, which causes or may cause, directly or indirectly, unjustified damage to the Reporting Person shall not be tolerated. By way of example, the following constitute breaches of the prohibition of retaliation:

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of location of place of work, reduction in wages, change in working hours;
- withholding of training;
- a negative performance assessment or employment reference;
- imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- failure to renew, or early termination of, a temporary employment contract;
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit;
- psychiatric or medical referrals.

6.2 Any retaliatory and discriminatory conduct may result in disciplinary proceedings and the consequent application of sanctions pursuant to Section No. 6.8.

6.3 Notwithstanding the above provision, the Reporting Person and other protected person may report to ANAC any retaliation they believe they have suffered.

6.4 The Reporting Person’s protection measures apply when the following conditions are met:

1) the Reporting Person had well-founded reason to believe that the information on Breaches was true and fell within the objective scope of application of this Appendix pursuant to paragraph 3;

2) the Report was made in compliance with the provisions of the Italian Whistleblowing Decree and, therefore, according to the provisions of this Appendix.

6.5 Where criminal liability of the Reporting Person for the offences of defamation or slander is established, including by a judgment of first instance, or civil liability of the Reporting Person for the same title, in cases of wilful misconduct or gross negligence, protection against retaliation is not guaranteed and a disciplinary sanction shall be applied to the Reporting Person in accordance with Paragraph 6.8.

6.6 A list of Third Sector entities that provide the Reporting Person with support measures is established at ANAC.

6.7 The support measures provided by Third Sector entities consist of cost-free information, assistance and advice about:

i. procedures for submitting Reports;

ii. protection measures offered by national and European Union legislative provisions;

iii. rights of the person involved, as well as;

iv. terms and conditions of access to legal aid.

6.8 Without prejudice to any other titles of liability, misconduct relevant under this Appendix, as well as violations thereof, may give rise to disciplinary proceedings and the consequent imposition of sanctions, in compliance with the provisions of applicable legislation, relevant collective bargaining, as well as internal regulations.

6.9 By way of example, the following constitute hypotheses liable to disciplinary sanction:

a) it is ascertained that the Report concerning Breaches that turned out to be unfounded was made through wilful misconduct or gross negligence;

b) conduct aimed at obstructing (as well as attempts to obstruct) the Report;

c) conduct and acts carried out in violation of the prohibition against retaliation under Paragraph 6.1;

d) violations of the obligations of confidentiality of the information referred to in the Report pursuant to paragraph 8;

e) failure to carry out follow-up activities (e.g., verification and analysis activities, etc.) of the Reports received;

f) failure to establish internal reporting channels;

g) failure to adopt procedures for making and managing Reports, or the adoption of procedures that do not comply with the Italian Whistleblowing Decree.

7 Keeping and managing records (Section 7.8 of the Policy)

7.1 Reports and the relevant documentation are kept and stored, by the **Committee** in paper and/or digital format – subject to the adoption of appropriate precautions to ensure their integrity and confidentiality – for as long as is necessary for the processing of the Report itself and, in any case, for no longer than five (5) years from the date of communication of the final outcome of the process, to grant protection of privacy, personal data, and security of network and information systems, in compliance with the confidentiality obligations set out in the Italian Whistleblowing Decree and the principles set out in the relevant laws and regulations on processing of personal data.

8 Confidentiality (Section 8 of the Policy)

8.1 The provisions contained in Section 8 of the Policy above also apply to the facilitator.

8.2 Within the course of disciplinary proceedings, the identity of the Reporting Person may not be disclosed, where the allegation of the disciplinary complaint is based on separate and additional investigations to the Report, even if consequent to the Report.

8.3 Where the complaint is based, in whole or in part, on the Report and the disclosure of the identity of the Reporting Person is indispensable for the defence of the person to whom the disciplinary complaint is made, the Report may be used for the purposes of the disciplinary proceedings only if the Reporting Person expressly consents to the disclosure of his or her identity. To this end, together with the request for consent, prior notice shall be given to the Reporting Person, by written communication, of the reasons for the disclosure of the confidential data. Same written notice shall be given in advance to the Reporting Person if, in the course of the process of managing the Report, the disclosure of the identity of the Reporting Person is also indispensable for the defence of person to whom the Breach is attributed.