MIZZI
ORGANISATION

Group Whistleblowing Policy

Table of Contents

Definitions

For the purpose of this Policy, the following terms shall be defined as follows:

- **"Act"**
  Malta's Protection of the Whistleblower Act, Chapter 527 of the Laws of Malta.

- **"Authority"**
  The entities prescribed to receive external disclosures, as listed in **Appendix III** to this Policy.

- **"Contract of Service"**
  An agreement whether oral or in writing, in any form, whereby a person binds himself/herself to render service to or do work for MO, in return for remuneration.

- **"Detrimental Action"**
  (a) Any action causing injury, loss or damage; and/or
  (b) Victimisation, intimidation or harassment; and/or
  (c) Occupational detriment; and/or
  (d) Prosecution relating to calumnious accusations; and/or
  (e) The institution of civil, criminal or disciplinary proceedings.

- **"Directive"**
  Directive (EU) 2019/1937 on the protection of persons who report breaches of European Union law.

- **"Employee"**
  (a) Any person who has entered into or works under a contract of service with MO and includes a contractor or a subcontractor who performs work or supplies a service or undertakes to perform any work or to supply services; or
  (b) Any person who has undertaken personally to execute any work or service for, and under the immediate direction and control of MO, including an outworker[1] but excluding work or services performed in a professional capacity to which an obligation of professional secrecy applies when such work or service is not regulated by a specific contract of service; or
  (c) Any former employee; or
  (d) Any person who is or was seconded to MO; or
  (e) Any candidate for employment who has acquired information concerning improper practices during the recruitment process or at another pre-contractual negotiating stage; or
  (f) Shareholders and persons belonging to the administrative, management or supervisory body of MO, including non-executive members, as well as volunteers and paid or unpaid trainees.

- **"GDPR"**
  The General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[1] An "outworker" means a person to whom articles, materials or services of any nature are given out by MO for the performance of any type of work or service where such work or service is to be carried out either in the home of the outworker or in some other premises not being under the control and management of that other person.

- **"Improper Practice"**

  An action or series of actions whereby:

  (a) A person has failed, is failing or is likely to fail to comply with any legal obligation to which he/she is subject; or
  (b) The health or safety of any individual has been, is being or is likely to be endangered; or
  (c) The environment has been, is being or is likely to be damaged; or
  (d) A corrupt practice[2] has occurred, is likely to occur or to have occurred; or
  (e) A criminal offence has been committed, is being committed or is likely to be committed; or
  (f) A miscarriage of justice has occurred, is occurring or is likely to occur; or
  (g) Bribery[3] has occurred, or is likely to occur or to have occurred; or
  (h) A person has failed, is failing or is likely to fail to comply with any legal obligation on public procurement to which he/she is subject; or
  (i) A person has failed, is failing or is likely to fail to comply with laws on financial services, products and markets, and prevention of money laundering and terrorist financing; or
  (j) A person has failed, is failing or is likely to fail to comply with product safety and compliance law; or
  (k) A person has failed, is failing or is likely to fail in ensuring transport safety; or
  (l) A person has failed, is failing or is likely to fail in ensuring radiation protection and nuclear safety; or
  (m) A person has failed, is failing or is likely to fail in ensuring a food and feed safety, animal health and welfare; or
  (n) A person has failed, is failing or is likely to fail to comply with any legal obligation on consumer protection to which he/she is subject; or
  (o) A person has failed, is failing or is likely to fail to comply with any legal obligation on protection of privacy and personal data, and security of network and information systems to which he/she is subject; or
  (p) A breach relating to fraud and any other illegal activities affecting the financial interests of the European Union has occurred or is likely to occur or to have occurred; or
  (q) A breach relating to the internal market (that is, an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured) including breaches of European 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 has occurred or is likely to occur or to have occurred; or
  (r) Information tending to show any matter falling within any one (1) of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

- **"IDPC"**

  The Office of the Information and Data Protection Commissioner of Malta.

- **"Mizzi Organisation" or "MO"**

  All companies and/or entities forming part of the Mizzi Organisation group, including Mizzi Organisation Limited, its subsidiaries and/or affiliates, which companies enter into a contract of service with an employee or employ or engage, or permit any other person in any manner to assist in the carrying on or conducting of its business, or which seeks to employ other persons.

[2] A corrupt practice has the same meaning as is assigned to it by article 6 of the Permanent Commission against Corruption Act.

[3] Bribery refers to any conduct in violation of articles 112 or 115 or of article 121 insofar as it extends the application of articles 112 and 115 of the Criminal Code.

- **“Occupational Detriment”**

  Any direct or indirect act or omission which occurs in a work-related context, which is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the Whistleblower and may include:

  (a) suspension, lay-off, dismissal or equivalent measures;
  (b) demotion or withholding of promotion;
  (c) transfer of duties, change of location of place of work, reduction in wages, change in working hours;
  (d) withholding of training;
  (e) a negative performance assessment or employment reference;
  (f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
  (g) coercion, intimidation, harassment or ostracism;
  (h) discrimination, disadvantageous or unfair treatment;
  (i) 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;
  (j) failure to renew, or early termination of, a temporary employment contract;
  (k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
  (l) 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;
  (m) early termination or cancellation of a contract for goods or services;
  (n) cancellation of a licence or permit;
  (o) psychiatric or medical referrals;
  (p) being subjected to any disciplinary action including for breach of ethics or confidentiality; and/or
  (q) being subjected to a term or condition of employment or retirement which is altered or kept altered to the disadvantage of the Whistleblower.

- **“Outworker”**

  A person to whom articles, materials or services of any nature are given out by MO for the performance of any type of work or service, and where such work or service is to be carried out either in the home of the outworker or in some other premises not being under the control and management of that other person.

- **“Policy”**

  This present Group Whistleblowing Policy.

- **“Whistleblower”**

  An employee who makes a disclosure through the internal or external reporting channels indicated in this Policy.

- **“Whistleblowing Reporting Officer” or “WRO”**

  The WRO refers to such officer appointed by MO as set out in **Appendix II** to this Policy.

- **“Whistleblowing Reports Unit” or “WRU”**

  The authorities prescribed to receive external disclosures as listed in **Appendix III** to this Policy.

1.0 Introduction

MO is committed to maintaining high ethical standards in all areas of work and practice based on the principles of honesty and integrity and conducts its business in line with these expectations and in accordance with all applicable laws and regulations.

The Directive creates a framework for persons who acquired information on certain breaches in connection with their work-related activities and serves to set minimum standards for the protection of persons reporting said breaches. The Directive was transposed into Maltese legislation by virtue of Act LXVII of 2021, amending the Act.

As part of this commitment, MO recognises the value and importance of its employees reporting suspected incidents and improper practices and strongly supports these disclosures. It is a cornerstone of this Policy that employees should feel comfortable in bringing forward any concerns in the knowledge that such concerns will be taken seriously, kept strictly confidential, and that there will be no detrimental action which may cause unjustified detriment to the person reporting said concern/improper practice.

This Policy is designed as a mechanism for individuals to raise any concerns which they may have about improper practices within the workplace in a respectable and effective manner and to provide Whistleblowers with information on how such concerns will be dealt with by MO. The objectives of this Policy shall therefore be as follows:

(a) To enable the Whistleblower to file disclosures through an internal reporting channel in a secure and confidential setting;
(b) To grant the person operating the internal reporting channel the necessary powers to be able to investigate any reports of improper practices in an effective manner and to ensure diligent follow-up;
(c) To protect the Whistleblower from potential risk of detrimental action which may ensue as a direct or indirect consequence of the disclosure; and
(d) To inform all employees of their rights and obligations insofar as these relate to whistleblowing and to ensure that all employees are aware of the Directive and the Act, and how these apply.

2.0 Purpose

The aim of this Policy is to improve the systems and procedures in place in terms of whistleblowing practices and enhance the overall integrity and performance of MO through transparent policies and effective procedures. It will also encourage all employees to report improper practices without any fear of retaliation and in a way that would allow the WRO to conduct an independent investigation into the matter.

3.0 Related documents

This Policy should be read in conjunction with the Employee Handbook/Manual in place within the respective MO company, but shall override any other Whistleblowing policies which may be in place at subsidiary level within MO.

4.0 Who is responsible for this Policy?

MO's Internal Audit Department has overall responsibility for the effective operation of this Policy. This Policy is reviewed on a biennial basis by the Group Chief Internal Auditor, in consultation with the respective third parties.

5.0 Who does this Policy apply to and what kinds of breaches may be reported?

This Policy shall apply to all Whistleblowers. In order for a disclosure to be considered to fall within the terms of this Policy, it must relate to an Improper Practice. Very minor or trivial matters shall not fall under the protection of this Policy.

For the avoidance of doubt, if a person is uncertain as to whether a breach would fall within the terms of this Policy or otherwise, such breaches should be reported nonetheless.

6.0 How to raise a concern

6.1 Internal disclosures

Whistleblowers wishing to file a disclosure shall do so through the internal reporting channel by completing the form attached hereto as **Appendix I** and submitting it directly and exclusively to the WRO as identified in **Appendix II**, by email as per the details outlined in **Appendix II**. Upon request by the Whistleblower, the WRO shall set up a physical meeting within a reasonable timeframe.

MO ensures to protect the confidentiality of the identity of the Whistleblower, as well as of any third party mentioned in the report. MO further ensures that non-authorised staff members shall not have access to such reports. When filing the disclosure, the Whistleblower should aim to provide sufficiently detailed information for the purposes of enabling the WRO to gather an understanding of the alleged breach in question.

Upon receipt of a disclosure, the WRO shall acknowledge the receipt of the report within seven (7) days of that receipt and shall then carry out an assessment on the accuracy of the allegations made in the report, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure, whilst keeping the Whistleblower informed of the progress of the assessment.

The WRO may ask the Whistleblower to provide further information during the course of the investigation. The WRO shall ensure to diligently follow-up on any disclosure filed by a Whistleblower and shall provide feedback on the outcome of the disclosure to the Whistleblower within a period not exceeding three (3) months from the date of the acknowledgement of receipt, or if no acknowledgement was sent to the Whistleblower, within a period not exceeding three (3) months from the expiry of the seven (7) day period after the report was made.

The Whistleblower may file an internal disclosure to the Chairman of the Board of Directors of MO if the Whistleblower has reasonable grounds to believe that the WRO is or may be involved in the alleged improper practice, or if the Whistleblower has reasonable grounds to believe that the WRO is, by reason of any relationship or association with a person who is or may be involved in the improper practice alleged in the disclosure, not a person to whom it is appropriate to make the disclosure.

6.2 External disclosures

The Whistleblower shall have the option of filing an external disclosure to the WRU of the relevant authority listed in **Appendix III** to this Policy.

This may be done after having first reported through internal reporting channels, or by directly reporting through external reporting channels in situations where the Whistleblower has reasonable grounds to believe that:

(a) The Chairman of the Board of Directors of MO is or may be involved in the improper practice alleged in the disclosure; or
(b) Immediate reference to the authority is justified by the urgency of the matter to which the disclosure relates, or some other exceptional circumstance; or
(c) At the time when the external disclosure is made, the Whistleblower will be subjected to an occupational detriment by MO if said Whistleblower makes an internal disclosure; or
(d) It is likely that evidence relating to the improper practice will be concealed or destroyed if he/she makes an internal disclosure; or
(e) Although an internal disclosure has previously been made, the Whistleblower has not been informed on the status of the matter disclosed or it is reasonably evident to the Whistleblower that there has been no action or recommended action on the matter to which the disclosure relates within a reasonable time from the making of the disclosure.

The external reporting channels will enable reporting in writing and orally and, upon request by the Whistleblower, reporting shall also be possible by means of a physical meeting within a reasonable timeframe.

Upon receipt of a disclosure, the respective authority listed in **Appendix III** must reach a conclusion as to whether it is appropriate for the disclosure to be made externally within forty-five (45) days after receiving the disclosure. If the authority concludes that a disclosure should not have been made externally, then it must within a reasonable time, not exceeding forty-five (45) days, notify the Whistleblower in writing that an internal disclosure must be made and that it will not be dealing with the disclosure any further. If on the other hand, the authority concludes that a disclosure has been properly made, it must within a reasonable time, notify the Whistleblower in writing of the status of the improper practice disclosed.

All authorities listed in **Appendix III** are bound to promptly, and in any event within seven (7) days of receipt of the external disclosure, acknowledge that receipt unless the Whistleblower explicitly requests otherwise or the WRU of the respective authority reasonably believes that acknowledging receipt of the disclosure would jeopardise the protection of the Whistleblower's identity.

The authority will ensure to diligently follow up on the report and will provide feedback to the Whistleblower within a reasonable timeframe not exceeding three (3) months, or six (6) months in duly justified cases. Following its assessment, the respective authority will communicate to the Whistleblower the final outcome of the investigation triggered by the report.

Competent authorities will ensure that where a report is received by staff members other than those responsible for handling reports, such staff members will be prohibited from disclosing any information that might identify the Whistleblower or the person concerned, and such

report will be promptly forwarded without modification, to the staff members responsible for handling reports.

6.3 Public disclosures

A public disclosure is a disclosure with respect to information on breaches available in the public domain, and this shall only be protected if an internal disclosure and an external disclosure in accordance with 6.1 and 6.2 above has already been made, but no appropriate action was taken in response to the report within the timeframes referred to.

A public disclosure shall be considered as a protected disclosure if the Whistleblower has reasonable grounds to believe that:

(a) the breach may constitute an imminent or manifest danger to the public interest, such as when there is an emergency situation or a risk of irreversible damage; or
(b) in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.

7.0 Protection measures

7.1 Eligibility for protection

Disclosures made by the Whistleblower shall be considered as protected disclosures under this Policy when the following conditions are satisfied:

(a) The Whistleblower had reasonable grounds to believe that the information on the Improper Practice/s disclosed was true at the time of disclosure and that such information fell within the scope of this Policy; and
(b) The Whistleblower disclosed either internally or externally, or made a public disclosure (i.e. made information on breaches available in the public domain), in accordance with the procedures mentioned above.

A disclosure shall not be considered as a protected disclosure where an employee knowingly discloses information which he/she knows or ought to reasonably know is false.

Disclosures made anonymously are not deemed to be protected disclosures. However, in cases where a public disclosure is made anonymously, and the Whistleblower is subsequently identified and suffers retaliation, said disclosure shall be considered to be a protected disclosure, provided the abovementioned conditions are satisfied.

7.2 Measures for protection against detrimental action

A Whistleblower who has made a protected disclosure shall be protected from any form of detrimental action. Where the Whistleblower files a protected disclosure, the Whistleblower shall not be liable to any civil or criminal proceedings or to a disciplinary proceeding for having made such disclosure. No immunity can be offered to a Whistleblower if he/she was the perpetrator or an accomplice to an improper practice.

7.3 Measures of support

The Whistleblower shall have access, as appropriate, to support measures, in particular the following:

(a) comprehensive and independent information and advice, which is easily accessible and free of charge, on procedures and remedies available, on protection against retaliation, and on the rights of the person concerned;
(b) effective assistance from competent authorities before any relevant authority involved in their protection against retaliation; and
(c) legal aid in criminal and in cross-border civil proceedings.

8.0 Confidentiality and data protection

8.1 Duty of confidentiality

The identity of the Whistleblower (or any other information from which the identity of the Whistleblower may directly or indirectly be deduced) is not to be disclosed to anyone beyond the authorised staff members competent to receive or follow up on reports, without the explicit consent of the Whistleblower.

8.2 Processing of personal data

Any processing of personal data carried out pursuant to this Policy (including the exchange or transmission of personal data both by MO and also by the competent authorities listed in **Appendix III**) shall be carried out in accordance with provisions set out in **Appendix IV** to this Policy.

Appendix I: Whistleblowing Disclosure Form

Whistleblower's Contact Information	
Name and Surname	
Position and Role	
Company Name	
Contact Number	
E-Mail Address	

Suspect's Information	
Name and Surname	
Position and Role	
Company Name	
Contact Number	
E-Mail Address	

Witness(es) Information (if any)	
Name and Surname	
Position and Role	
Company Name	
Contact Number	
E-Mail Address	

Name and Surname	
Position and Role	
Company Name	
Contact Number	
E-Mail Address	

Name and Surname	
Position and Role	
Company Name	
Contact Number	
E-Mail Address	

If there are more than three witnesses, please give their details on as many pages as necessary.

Disclosure of Improper Practice

Briefly **describe** the alleged breach and **how** you came to know about it. Specify **what, who, when, where and how**. If there is more than one allegation, number each allegation and use as many pages as necessary.

Describe the alleged breach	
What is the nature of the breach?	
Who committed the breach?	
When did it happen and when did you notice it?	
Where did it happen?	
Is there any evidence that you can provide? ***NOTE: YOU SHOULD NOT ATTEMPT TO OBTAIN EVIDENCE FOR WHICH YOU DO NOT HAVE A RIGHT OF ACCESS SINCE WHISTLEBLOWERS ARE 'DISCLOSING PARTIES' AND NOT 'INVESTIGATORS'***	
Other person(s) involved other than the suspect(s) stated above	
Any other details or information which would assist in the investigation	
Any additional comments	

Please note that you may be called upon to assist in the investigation, if required.

Date	Signature (Optional)

Appendix II: WRO

MO appointed the following independent officials as WRO:

- **Mr Charles J. Farrugia**
  MO/MOF Audit Committee Chairman
  Email: WRO@mizzi.com.mt

- **Mr Giancarlo Millo**
  Group Chief Internal Auditor
  Email: WRO@mizzi.com.mt

Appendix III: Authorities prescribed to receive external disclosures

The following is a list of the authorities prescribed to receive external disclosures as extracted from the Act, First Schedule, Part 1 – Private Sector:

Authority	Description of Matters	Contact Details
Auditor General	Failure to observe laws, rules and regulations relating to public finance and misuse of public resources.	National Audit Office Notre Dame Ravelin Floriana FRN 1601 Malta Email: nao.malta@gov.mt Phone: (+356) 2205 5555
Commissioner for Revenue	Income tax, corporation tax, capital gains tax, stamp duties, national insurance contributions, value added tax or "revenue acts" as defined in the Commissioner for Revenue Act.	Taxpayer Service servizz.gov Block 4 Vincenzo Dimech Street Floriana FRN 1900 Malta Email: servizz@gov.mt Call Centre: (+356) 153
Commissioner for Voluntary Organisations	Activities of a voluntary organisation.	Office of the Commissioner for Voluntary Organisations Sqaq Sajjan, Blata l-Bajda Hamrun HMR 1680 Malta Email: vo@gov.mt / inclusion@gov.mt Phone: (+356) 2744 0388
Financial Intelligence Analysis Unit	Money laundering or financing of terrorism in terms of the Prevention of Money Laundering Act.	Financial Intelligence Analysis Unit 65C, Tower Street Birkirkara BKR 4012 Malta Phone: (+356) 2123 1333
Malta Financial Services Authority	The business of credit and financial institutions, the business of insurance and the activities of insurance intermediaries, the provision of investment services and collective investment schemes, pensions and retirement funds, regulated markets, central securities depositories, the carrying out of trustee business either in a professional or a personal capacity and such other areas of activity or services as may be placed from time to time under the supervisory and	Malta Financial Services Authority Triq l-Imdina, Zone 1 Central Business District Birkirkara CBD 1010 Malta Phone: (+356) 2144 1155

	regulatory competence of the Malta Financial Services Authority.	
Ombudsman	i) Conduct involving substantial risk to public health or safety or the environment that would if proved, constitute a criminal offence; and ii) All matters which constitute improper practices and which are not designated to be reported to any other authority.	Office of the Ombudsman 11, St Paul Street Valletta VLT 1210 Malta Email: office@ombudsman.org.mt Phone: (+356) 2248 3200
Permanent Commission Against Corruption	Corrupt practices.	Permanent Commission Against Corruption 17, Door 19 Vincenti Building Strait Street Valletta VLT 1432 Malta Email: pcac.pcac@gov.mt Phone: (+356) 2327 9291

Appendix IV: Data protection & processing considerations

In accordance with Articles 13 and 14 of the GDPR and the Maltese Data Protection Act, Chapter 586 of the Laws of Malta (together with its subsidiary legislation), in relation to the management of the internal whistleblowing reporting channel as set out in this Policy, MO hereby informs all relevant Data Subjects, that any information and personal data provided through, or requested by said internal whistleblowing reporting channel will be processed by the Data Controller in the manner set out below. For the avoidance of doubt, all terms defined in the Policy shall be applicable throughout this Appendix. Additionally, the term 'Data Subject' shall refer to (i) the Whistleblower; and (ii) any other person mentioned in the report filed by the Whistleblower. The term 'Data Controller' shall refer to (i) the WRO; and (ii) to the extent that the WRO shares any data with MO, MO shall also be considered as a Data Controller.

1) Any processing of personal data carried out by MO or by the Data Controller pursuant to this Policy (including the exchange or transmission of personal data) shall be carried out in accordance with the following:

   (a) The GDPR;
   (b) The Data Protection Act, Chapter 586 of the Laws of Malta;
   (c) The Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations, Subsidiary Legislation 586.08 of the Laws of Malta; and
   (d) Other relevant legislation.

2) Any personal data processed by the Data Controller in terms of this Policy will be limited to the personal data which is strictly and objectively necessary to verify the legitimacy of the allegations made, including the Data Subject's name, surname, mailing address, telephone or mobile number and/or email address.

3) Personal data will be processed both manually and with the aid of electronic or automated means suitable to guarantee the highest security and confidentiality in compliance with the provisions of the above-mentioned laws.

4) By accessing and using the whistleblowing reporting systems set out in this Policy, the Data Subject agrees to the processing of his/her personal data for the purposes indicated in this Appendix.

5) Personal data which is manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay. The Data Controller to whom a protected disclosure is made or referred must not disclose information that identifies or may lead to the identification of the Data Subject, unless the Data Subject expressly consents in writing to the disclosure of that information. No court may order the disclosure of the identity of any Data Subject without his/her consent.

6) In cases where a Data Controller receives information on breaches that includes trade secrets (as defined under Article 2 of the Trade Secrets Act), the Data Controller shall not use or disclose those trade secrets for purposes going beyond what is necessary for proper follow-up.

7) The Data Controller shall keep records of every report received, provided that, reports shall be stored for no longer than is necessary and proportionate in order to comply with the requirements imposed by the Act or by any other law.

8) Where a recorded telephone line or another recorded voice messaging system is used for disclosing, subject to the consent of the Data Subject, the Data Controller shall have the right to document the oral reporting in one (2) of the following ways:

   (a) By making a recording of the conversation in a durable and retrievable form; or
   (b) Through a complete and accurate transcript of the conversation prepared by the staff members responsible for handling the report.

   Provided that, in such a case, the Data Controller shall offer the Data Subject the opportunity to check, rectify and confirm the transcript of the call by signing said transcript.

9) Where an unrecorded telephone line or another unrecorded voice messaging system is used for disclosing, the Data Controller shall have the right to document the oral disclosure in the form of accurate minutes of the conversation written by the staff members responsible for handling the disclosure.

   Provided that, in such a case, the Data Controller shall offer the Data Subject the opportunity to check, rectify and confirm the minutes by signing said minutes.

10) In cases where a Data Subject requests a meeting with the Data Controller for the purposes of disclosing an improper practice as per the procedures set out in this Policy, the Data Controller shall ensure, subject to the consent of the Data Subject, that complete and accurate records of the meeting are kept in a durable and retrievable form. The Data Controller shall have the right to document the meeting in one of the following ways:

    (a) By making a recording of the conversation in a durable and retrievable form; or
    (b) Through accurate minutes of the meeting prepared by the staff members responsible for handling the report.

    Provided that, in such a case, the Data Controller shall offer the Data Subject the opportunity to check, rectify and confirm the minutes of the meeting by signing said minutes.

11) As a general rule, any personal data processed under this Policy will be stored and processed within the European Union (EU), and/or European Economic Area (EEA), and/or any other non-EEA country deemed by the European Commission to offer an adequate level of protection as listed here.

12) MO guarantees to use all reasonable efforts to safeguard the confidentiality of any and/or all personal data that may be processed under this Policy and to regularly review and enhance its technical, physical and managerial procedures so as to ensure that said personal data is protected from unauthorised access, improper use or disclosure, unauthorised modification, and/or unlawful destruction or accidental loss.

13) Despite the above, MO cannot guarantee that a data transmission or a storage system can ever be 100% secure and MO shall accept no responsibility or liability whatsoever for the security of any data collected under this Policy while in transit through the Internet.

14) Data Subjects have a number of rights that are applicable under certain conditions and in certain circumstances, including the following:

    (a) Right of access to his/her personal data;
    (b) Right to ask the Data Controller to rectify inaccurate personal data concerning the individual in question;
    (c) Right to have the Data Controller erase his/her personal data ('right to be forgotten');
    (d) Right to ask the Data Controller to restrict (that is, store but not further process) his/her personal data;
    (e) Right to ask the Data Controller to provide his/her personal data to him/her in a structured, commonly used, machine-readable format, or (where technically feasible) to have it 'ported' directly to another data controller ('right to data portability');
    (f) Right to object to the Data Controller's processing his/her personal data on the grounds of the Data Controller's legitimate interest; and
    (g) Right to lodge a complaint with the Maltese Information and Data Protection Commissioner.

15) Data Subjects wishing to lodge a complaint with the Maltese Information and Data Protection Commissioner may do so through the online Complaint Form which can be accessed here. For any other queries, Data Subjects may contact the Information and Data Protection Commissioner on idpc.info@idpc.org.mt or (+356) 2328 7100.

Version history

Version	Change Summary	Issue Date
v1-Proposed	First version proposed for approval by MO/MOF Audit Committee	25/11/2021
v2-Proposed	Second version proposed for approval by MO/MOF Audit Committee following consultation with GVZH Advocates to ensure compliance with latest whistleblowing legislation	13/04/2022
v1	MO Group Whistleblowing Policy approved by MO Main Board	06/09/2022