GUIDELINES ON PREPARING A WHISTLEBLOWER POLICY

[Version 4.0, 30-05-2024]

Employers in the private sector who are required to establish an internal reporting channel[[1]](#footnote-1) are by national acts implementing the Whistleblower Directive required to keep written documentation for the establishment of the internal reporting channel and the related procedures. That document can be referred to as a ‘Whistleblower Policy’.

As we must align our in-house practices, regarding the screening of reports, to all customers, Compliance Partners has made a Whistleblower Policy from a one-size-fits-all-concept. It is an obligation for the provision of our Whistleblower Service, that customers use this template as their Whistleblower Policy. If you want to discuss changes, please contact your assigned Effortless Compliance Officer (ECO).

In these guidelines, you can see our template for the Whistleblower Policy (Section 1) and an example of the Whistleblower Policy in action (Section 2).

To use the template, you just need to copy the template (all of Section 1), fill in the ‘blank spots’ marked with yellow in the template, and remove the text marked with red. Under Section 3, you have to choose a clause depending on which jurisdiction your organization resides in. Please contact your assigned ECO, if you have any questions.

[IF CHANGES ARE MADE TO THE TEMPLATE OR ANOTHER TEMPLATE IS USED, COMPLIANCE PARTNERS CANNOT GUARANTEE THE PROVISION OF THE WHISTLEBLOWER SERVICE. CHANGES AND OTHER TEMPLATES ARE USED AT OWN RESPONSIBILITY.]

# **TEMPLATE FOR WHISTLEBLOWER POLICY**

**WHISTLEBLOWER POLICY FOR [NAME OF ORGANIZATION]**

*Version [XX], Last update on [XX-XX-XXXX]*

*Section 1*

**Background and Purpose**

1. [NAME OF THE ORGANIZATION] (referred to as “the Organization”) is establishing an internal reporting channel available for the use of our employees, among others, in accordance with the national act implementing the Directive (EU) 2019/1937, on the protection of persons who report breaches of EU law (referred to as “the Whistleblower Directive”).
2. The internal reporting channel is an independent channel where employees, among others, can report information on breaches, etc., in the Organization.
3. This Whistleblower Policy describes the personal scope of application (Section 2), the material scope of application (Section 3), submitting reports (Section 4), the operation of the reporting channel (Section 5), the confidentiality measures (Section 6), the procedures for receiving reports (Section 7), the procedures for follow-up (Section 8), the procedures for feedback (Section 9), record keeping of reports (Section 10), and the procedures for reporting externally (Section 11).
4. The operator of the internal reporting channel, Compliance Partners ApS, provides persons concerned how their personal data is processed via the ‘Privacy Notice’, in accordance with Articles 13 and 14 of Regulation 2016/679 (General Data Protection Regulation). The reporting person is informed after submitting the report. In addition, the Privacy Notice can be found on Compliance Partners’ website via this [link](https://usercontent.one/wp/www.compliancepartners.com/wp-content/uploads/2024/03/Privacy-Notice.pdf?media=1715162823).
5. The Organization is responsible for providing clear and easily accessible information to employees, among others, about the procedures for reporting internally. The Organization has provided employees, among others, with the appropriate information relating to the use of the internal and external reporting channels at: [INSERT REFERENCE TO THE PHYSICAL PLACE WHERE EMPLOYEES, AMONG OTHERS, CAN ACCESS INFORMATION RELATED TO THE PROCEDURE TO REPORT].

*Section 2*

**Personal Scope of Application**

1. The internal reporting channel is available for the Organization’s employees, including fixed-term, part-time, and seasonal employees, and in addition self-employed, the shareholders and the persons belonging to the administrative, management, or supervisory body of the Organization, including non-executive members, as well as volunteers and paid or unpaid trainees, and any persons working under the supervision and direction of contractors, subcontractors and suppliers, who are in contact with the Organization in the context of work-related activities (‘whistleblowers’).
2. Furthermore, the internal reporting channel is available for whistleblowers who acquire information on breaches, etc., in a work-based relationship that has since ended or is yet to begin, such as during a recruitment process or other pre-contractual negotiations.
3. Whistleblowers can report information on breaches, etc., concerning the persons mentioned in Sections 2(1) and 2(2).
4. Whistleblowers can report information on breaches, etc., without disclosing their identity, that is, whistleblowers can choose to stay anonymous.

*Section 3*

**Material Scope of Application**

3.A. USE THIS SECTION IF THE ORGANIZATION’S HEADQUARTERS IS IN DENMARK

1. There can be reported information regarding the following subjects, which is a non-exhaustive list of examples:
	1. breaches related to the regulation mentioned in Part I in the Annex to the Whistleblower Directive, in the area of public procurement, financial services, products and markets, 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;
	2. breaches affecting financial interests;
	3. breaches relating to the internal market, including competition and state aid rules, and corporate tax rules;
	4. severe breaches and other severe matters as violations of the Danish Criminal Act (No. 434 of 25-04-2024), including bribery, document forgery, theft, embezzlement, fraud, mandate fraud, and extortion, violations of confidentiality obligations, the Bookkeeping Act (No. 700 of 24-05-2022), the Freight Transport Act (No. 327 of 23-03-2024), the Aviation Act (No. 118 of 31-01-2024), where there is a legal obligation to act, sexual harassment and gross harassment, violation of professional standards that could cause a risk to the health of persons, serious errors related to it-operations, minor difficulties in cooperation that involve major risks, and gross or repeated violations of internal rules.
2. There can NOT be reported information regarding the following subjects, which is a non-exhaustive list of examples:
	1. breaches of procurement rules, involving defence or security aspects, unless covered by the relevant acts of the EU;
	2. classified information under the Danish Ministry of Justice’s ‘Security Circular’ (No. 10338 of 17-12-2014);
	3. information under the privilege of legal professionals in accordance with the Administration of Justice Act (No. 250 of 03-04-2024);
	4. information under the privilege of healthcare professionals in accordance with the Healthcare Act (No. 247 of 03-12-2024);
	5. confidential information about deliberation and voting of the courts;
	6. cases within the criminal justice system;
	7. information about the whistleblower’s own employment relationship, unless the information is regarding severe breaches or other severe matters;
	8. breaches of a less serious nature, such as rules about sick leave, alcohol, attire, private use of office supplies, personnel-related conflicts in the workplace, and corporation issues between two or more employees.

3.B. USE THIS SECTION IF THE ORGANIZATION’S HEADQUARTERS IS IN SWEDEN

1. There can be reported information regarding the following subjects, which is a non-exhaustive list of examples:
	1. breaches related to the regulation mentioned in Part I in the Annex to the Whistleblower Directive, in the area of public procurement, financial services, products and markets, 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;
	2. breaches affecting financial interests;
	3. breaches relating to the internal market, including competition and state aid rules, and corporate tax rules;
	4. misconduct that there is a public interest in bringing to light;
	5. misconduct that consists of an act or omission that conflicts with the aim or purpose of the acts mentioned in Part I in the Annex to the Whistleblower Directive.
2. There can NOT be reported information regarding the following subjects, which is a non-exhaustive list of examples:
	1. breaches of procurement rules, involving defence or security aspects, unless covered by the relevant acts of the EU;
	2. classified information under the Swedish Security Protection Act (2018:585);
	3. information relating to national security in the activities of authority in the field of security or defence.

3.C. USE THIS SECTION IF THE ORGANIZATION’S HEADQUARTERS IS IN FINLAND

1. There can be reported information regarding the following subjects, which is a non-exhaustive list of examples:
	1. acts or omissions that are either a criminal offence, can lead to an administrative sanction of criminal nature, or can jeopardize the achievement of the public interest objectives, related to the regulation mentioned in Part I in the Annex to the Whistleblower Directive, in the area of public procurement, financial services, products and markets, 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;
	2. breaches affecting financial interests;
	3. breaches relating to the internal market, including competition and state aid rules, and corporate tax rules;
	4. breaches of legislation enacted to protect consumers.
2. There can NOT be reported information regarding the following subjects, which is a non-exhaustive list of examples:
	1. breaches of procurement rules, involving defence or security aspects, unless covered by the relevant acts of the EU;
	2. breaches of specific provisions in the Finish Medicine Act (395/1987), the Act on the Use of Human Organs, Tissues, and Cells for Medical Purposes (101/2001), the Act on Cross-border Healthcare (1201/2013);
	3. breaches related to classified information under the Act on Information Management in Public Administration (906/2019) and the Act on International Information Security Obligations (588/2004);
	4. information under the privilege of healthcare professionals in accordance with the Act on Healthcare Professionals (559/1994) or the Private Healthcare Act (152/1990);
	5. information under the privilege of legal professionals in accordance with the Code of Judicial Procedure, etc.;
	6. information about the confidentiality of a court’s decision-making, if the matter is specifically provided for in the Act on the Openness of Proceedings in General Courts (370/2007) or the Act on the Openness of Proceedings in Administrative Courts (381/2007);
	7. in cases where a person has given his or her informed consent to be listed as a source of information or registered as such in databases managed by law enforcement authorities.

3.D. USE THIS SECTION IF THE ORGANIZATION’S HEADQUARTERS IS IN GERMANY

1. There can be reported information regarding the following subjects, which is a non-exhaustive list of examples:
	1. breaches that are punishable;
	2. breaches that are subject to fines where the relevant provision serves to protect life, limb or health, or to protect the rights of employees or their representative;
	3. breaches related to the regulation mentioned in Part I in the Annex to the Whistleblower Directive, in the area of public procurement, financial services, products and markets, 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;
	4. breaches affecting financial interests;
	5. breaches relating to the internal market, including competition and state aid rules, and corporate tax rules;
	6. breaches who regulate the rights of shareholders of limited liability companies;
	7. breaches related to the audit of financial statements for companies of public interest;
	8. breaches related to accounting, including bookkeeping, of companies that are capital market-oriented, credit institutions, financial services institutions, securities institutions, insurance companies, and pension funds;
	9. breaches of civil servants’ obligation under the German Constitution.
2. There can NOT be reported information regarding the following subjects, which is a non-exhaustive list of examples:
	1. information concerning national security or essential security interests of the state;
	2. information from federal or state intelligence services or from authorities or other public bodies of the federal or state governments;
	3. breaches of procurement rules, involving defence or security aspects, unless covered by the relevant acts of the EU;
	4. information covered by a duty of secrecy or confidentiality.

*Section 4*

**Submitting Reports**

1. Whistleblowers can submit reports in writing via an online platform, available at: [INSERT LINK LISTED AT THE TOP OF THE WELCOME LETTER]. The channel does not enable oral reporting.

*Section 5*

**Operation of the Reporting Channel**

1. The internal reporting channel is operated externally by Compliance Partners, which has designated a department to operate the internal reporting channel (‘the Effortless Compliance Team’). Compliance Partners has provided a written guarantee to live up to safeguards and requirements provided in the national act implementing the Whistleblower Directive, of respect for independence, confidentiality, data protection, and secrecy.

*Section 6*

**Confidentiality Measures**

1. The internal reporting channel is designed, established, and operated in a secure manner that ensures that the confidentiality of the identity of the whistleblower and other persons mentioned in the report is protected, and prevents access thereto by non-authorized staff members by implementing the following measures:
	1. only authorized staff members of the Effortless Compliance Team have access to the information in the report;
	2. all information from reports is subject to a special duty of confidentiality, meaning that the identity of the reporting person or any other information from which the identity of the reporting person may be directly or indirectly deduced, must not be disclosed to anyone beyond the authorized staff members of the Effortless Compliance Team, without the explicit consent of the whistleblower;
	3. authorized staff members of the Effortless Compliance Team are trained in handling confidential information and are subject to Compliance Partners’ internal guidelines about handling confidential information;
	4. the online platform is subject to data security requirements that protect the data, including, among others, no logging of the users’ IP addresses, the metadata is removed from all uploaded files, and data transmission and storage is encrypted.
2. Information from reports may be disclosed in the context of investigations by national authorities or judicial proceedings where this is a necessary and proportionate obligation imposed by EU or national law. The disclosure shall be subject to appropriate safeguards under the applicable EU and national rules. Whistleblowers shall be informed before their identity is disclosed unless such information would jeopardize the related investigations or judicial proceedings.

*Section 7*

**Procedures for Receiving Reports**

1. Following the requirements set out in the national act implementing the Whistleblower Directive, upon receiving a report from the internal reporting channel, the Effortless Compliance Team will:
	1. send an acknowledgment of receipt of the report to the whistleblower within 7 (seven) days of that receipt;
	2. assessing whether the report falls under the scope of the national act implementing the Whistleblower Directive, in accordance with Compliance Partners’ internal guidelines;
	3. assessing whether the report is suitable for further processing, in accordance with Compliance Partners’ internal guidelines;
	4. assessing the accuracy of the allegations made in the report;
	5. maintaining communication with the whistleblower and, where necessary, asking for further information from and providing feedback.
2. If the Effortless Compliance Team has assessed that the report falls outside the scope of the national act implementing the Whistleblower Directive or is not suitable for further processing, the whistleblower will be informed about the dismissal of the report. Depending on the specific circumstances, the whistleblower might be directed to raise the matter in question elsewhere, such as an external reporting channel.

*Section 8*

**Procedures for Follow-up**

1. If it has been assessed that the report falls under the scope of the national act implementing the Whistleblower Directive, and the report is deemed suitable for further processing, the Effortless Compliance Team will, with the explicit consent of the whistleblower, transmit the report to the relevant contact person(s) in the Organization.
2. If the whistleblower does not consent to the transmission of the report, and if the circumstances so dictate, the Effortless Compliance Team can transmit a general report, without jeopardizing the identity of the whistleblower or any other information from which the identity may be directly or indirectly deduced.
3. The Effortless Compliance Team ensures that the relevant contact person(s) in the Organization has no conflicts of interest in relation to the report. If this is the case, the report will be transmitted to another person in the Organization, whom the Effortless Compliance Teams deem competent.
4. Once the relevant contact person(s) in the Organization has received a report, the person(s) must diligently follow up on the report, which entails assessing the accuracy of the allegations made in the report and, where relevant, to address the breach reported. Follow-up measures are the responsibility of the Organization.
5. Follow-up can, for example, consist of the Organization taking the following measures:
	1. filing a report to the police or other relevant authorities;
	2. initiating an internal investigation for sanctions in an employment relationship, such as warning or dismissal;
	3. initiating an investigation for sanctions in other contractual relationships, such as termination;
	4. dismissal of the report.

*Section 9*

**Procedures for Feedback**

1. Within 3 (three) months after the initial confirmation of receipt, the Effortless Compliance Team shall, on the basis of a dialogue between the Effortless Compliance Team and the relevant contact person(s) in the Organization, provide feedback to the whistleblower. If the appropriate follow-up measures have not been determined after this period of time, the whistleblower should be informed about when feedback could be expected.
2. Feedback means that the whistleblower must be informed of what measures the Organization has taken or has intended to take, including the reasoning behind the chosen follow-up measures.

*Section 10*

**Record Keeping of Reports**

1. In compliance with the confidentiality requirements provided for in the national act implementing the Whistleblower Directive, Compliance Partners keep records of every report received. Reports are kept on the online platform. Reports shall be stored for no longer than it is necessary and proportionate, in accordance with Compliance Partners’ time limits for the erasure of personal data.

*Section 11*

**Procedures for Reporting Externally**

1. The Organization is responsible for providing clear and easily accessible information to whistleblowers, about the procedures for reporting externally to competent authorities and, where relevant, to institutions, bodies, offices, or agencies of the EU. The Organization has, in addition to the below, provided this information in accordance with Section 1(5).
2. Whistleblowers can report externally to the following authorities:
	1. At [NAME OF AUTHORITY] breaches, etc., can be reported relating to [INSERT A SHORT DESCRIPTION OF THE SCOPE OF THE EXTERNAL REPORTING CHANNEL]. More information regarding this external reporting channel can be found here: [INSERT LINK TO INFORMATION ON THE EXTERNAL REPORTING CHANNEL].
	2. [COPY AND INSERT THE TEXT ABOVE IF THERE IS MORE EXTERNAL REPORTING CHANNELS].
3. Whistleblowers have freedom of choice regarding whether to report internally or externally.

# **EXAMPLE OF WHISTLEBLOWER POLICY**

**WHISTLEBLOWER POLICY FOR HIGH-TECH A/S**

*Version 1.0, Last update on 01-12-2023*

*Section 1*

**Background and Purpose**

1. High-Tech A/S (referred to as “the Organization”) is establishing an internal reporting channel available for the use of our employees, among others, in accordance with the national act implementing the Directive (EU) 2019/1937, on the protection of persons who report breaches of EU law (referred to as “the Whistleblower Directive”).
2. The internal reporting channel is an independent channel where employees, among others, can report information on breaches, etc., in the Organization.
3. This Whistleblower Policy describes the personal scope of application (Section 2), the material scope of application (Section 3), submitting reports (Section 4), the operation of the reporting channel (Section 5), the confidentiality measures (Section 6), the procedures for receiving reports (Section 7), the procedures for follow-up (Section 8), the procedures for feedback (Section 9), record keeping of reports (Section 10), and the procedures for reporting externally (Section 11).
4. The operator of the internal reporting channel, Compliance Partners ApS, provides persons concerned how their personal data is processed via the ‘Privacy Notice’, in accordance with Articles 13 and 14 of Regulation 2016/679 (General Data Protection Regulation). The reporting person is informed after submitting the report. In addition, the Privacy Notice can be found on Compliance Partners’ website via this [link](https://usercontent.one/wp/www.compliancepartners.com/wp-content/uploads/2024/03/Privacy-Notice.pdf?media=1715162823).
5. The Organization is responsible for providing clear and easily accessible information to employees, among others, about the procedures for reporting internally. The Organization has provided employees, among others, with the appropriate information relating to the use of the internal and external reporting channels at: [www.intranet.com](http://www.intranet.com).

*Section 2*

**Personal Scope of Application**

1. The internal reporting channel is available for the Organization’s employees, including fixed-term, part-time, and seasonal employees, and in addition self-employed, the shareholders and the persons belonging to the administrative, management, or supervisory body of the Organization, including non-executive members, as well as volunteers and paid or unpaid trainees, and any persons working under the supervision and direction of contractors, subcontractors and suppliers, who are in contact with the Organization in the context of work-related activities (‘whistleblowers’).
2. Furthermore, the internal reporting channel is available for whistleblowers who acquire information on breaches, etc., in a work-based relationship that has since ended or is yet to begin, such as during a recruitment process or other pre-contractual negotiations.
3. Whistleblowers can report information on breaches, etc., concerning the persons mentioned in Sections 2(1) and 2(2).
4. Whistleblowers can report information on breaches, etc., without disclosing their identity, that is, whistleblowers can choose to stay anonymous.

*Section 3*

**Material Scope of Application**

1. There can be reported information regarding the following subjects, which is a non-exhaustive list of examples:
	1. breaches related to the regulation mentioned in Part I in the Annex to the Whistleblower Directive, in the area of public procurement, financial services, products and markets, 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;
	2. breaches affecting financial interests;
	3. breaches relating to the internal market, including competition and state aid rules, and corporate tax rules;
	4. severe breaches and other severe matters as violations of the Danish Criminal Act (No. 434 of 25-04-2024), including bribery, document forgery, theft, embezzlement, fraud, mandate fraud, and extortion, violations of confidentiality obligations, the Bookkeeping Act (No. 700 of 24-05-2022), the Freight Transport Act (No. 327 of 23-03-2024), the Aviation Act (No. 118 of 31-01-2024), where there is a legal obligation to act, sexual harassment and gross harassment, violation of professional standards that could cause a risk to the health of persons, serious errors related to it-operations, minor difficulties in cooperation that involve major risks, and gross or repeated violations of internal rules.
2. There can NOT be reported information regarding the following subjects, which is a non-exhaustive list of examples:
	1. breaches of procurement rules, involving defence or security aspects, unless covered by the relevant acts of the EU;
	2. classified information under the Danish Ministry of Justice’s ‘Security Circular’ (No. 10338 of 17-12-2014);
	3. information under the privilege of legal professionals in accordance with the Administration of Justice Act (No. 250 of 03-04-2024);
	4. information under the privilege of healthcare professionals in accordance with the Healthcare Act (No. 247 of 03-12-2024);
	5. confidential information about deliberation and voting of the courts;
	6. cases within the criminal justice system;
	7. information about the whistleblower’s own employment relationship, unless the information is regarding severe breaches or other severe matters;
	8. breaches of a less serious nature, such as rules about sick leave, alcohol, attire, private use of office supplies, personnel-related conflicts in the workplace, and corporation issues between two or more employees.

*Section 4*

**Submitting Reports**

1. Whistleblowers can submit reports in writing via an online platform, available at: [www.whistleportal.com](http://www.whistleportal.com). The channel does not enable oral reporting.

*Section 5*

**Operation of the Reporting Channel**

1. The internal reporting channel is operated externally by Compliance Partners ApS, which has designated a department to operate the internal reporting channel (‘the Effortless Compliance Team’). Compliance Partners has provided a written guarantee to live up to safeguards and requirements provided in the national act implementing the Whistleblower Directive, of respect for independence, confidentiality, data protection, and secrecy.

*Section 6*

**Confidentiality Measures**

1. The internal reporting channel is designed, established, and operated in a secure manner that ensures that the confidentiality of the identity of the whistleblower and other persons mentioned in the report is protected, and prevents access thereto by non-authorized staff members by implementing the following measures:
	1. only authorized staff members of the Effortless Compliance Team have access to the information in the report;
	2. all information from reports is subject to a special duty of confidentiality, meaning that the identity of the reporting person or any other information from which the identity of the reporting person may be directly or indirectly deduced, must not be disclosed to anyone beyond the authorized staff members of the Effortless Compliance Team, without the explicit consent of the whistleblower;
	3. authorized staff members of the Effortless Compliance Team are trained in handling confidential information and are subject to Compliance Partners’ internal guidelines about handling confidential information;
	4. the online platform is subject to data security requirements that protect the data, including, among others, no logging of the users’ IP addresses, the metadata is removed from all uploaded files, and data transmission and storage is encrypted.
2. Information from reports may be disclosed in the context of investigations by national authorities or judicial proceedings where this is a necessary and proportionate obligation imposed by EU or national law. The disclosure shall be subject to appropriate safeguards under the applicable EU and national rules. Whistleblowers shall be informed before their identity is disclosed unless such information would jeopardize the related investigations or judicial proceedings.

*Section 7*

**Procedures for Receiving Reports**

1. Following the requirements set out in the national act implementing the Whistleblower Directive, upon receiving a report from the internal reporting channel, the Effortless Compliance Team will:
	1. send an acknowledgment of receipt of the report to the whistleblower within 7 (seven) days of that receipt;
	2. assessing whether the report falls under the scope of the national act implementing the Whistleblower Directive, in accordance with Compliance Partners’ internal guidelines;
	3. assessing whether the report is suitable for further processing, in accordance with Compliance Partners’ internal guidelines;
	4. assessing the accuracy of the allegations made in the report;
	5. maintaining communication with the whistleblower and, where necessary, asking for further information from and providing feedback.
2. If the Effortless Compliance Team has assessed that the report falls outside the scope of the national act implementing the Whistleblower Directive or is not suitable for further processing, the whistleblower will be informed about the dismissal of the report. Depending on the specific circumstances, the whistleblower might be directed to raise the matter in question elsewhere, such as an external reporting channel.

*Section 8*

**Procedures for Follow-up**

1. If it has been assessed that the report falls under the scope of the national act implementing the Whistleblower Directive, and the report is deemed suitable for further processing, the Effortless Compliance Team will, with the explicit consent of the whistleblower, transmit the report to the relevant contact person(s) in the Organization.
2. If the whistleblower does not consent to the transmission of the report, and if the circumstances so dictate, the Effortless Compliance Team can transmit a general report, without jeopardizing the identity of the whistleblower or any other information from which the identity may be directly or indirectly deduced.
3. The Effortless Compliance Team ensures that the relevant contact person(s) in the Organization has no conflicts of interest in relation to the report. If this is the case, the report will be transmitted to another person in the Organization, whom the Effortless Compliance Teams deem competent.
4. Once the relevant contact person(s) in the Organization has received a report, the person(s) must diligently follow up on the report, which entails assessing the accuracy of the allegations made in the report and, where relevant, to address the breach reported. Follow-up measures are the responsibility of the Organization.
5. Follow-up can, for example, consist of the Organization taking the following measures:
	1. filing a report to the police or other relevant authorities;
	2. initiating an internal investigation for sanctions in an employment relationship, such as warning or dismissal;
	3. initiating an investigation for sanctions in other contractual relationships, such as termination;
	4. dismissal of the report.

*Section 9*

**Procedures for Feedback**

1. Within 3 (three) months after the initial confirmation of receipt, the Effortless Compliance Team shall, on the basis of a dialogue between the Effortless Compliance Team and the relevant contact person(s) in the Organization, provide feedback to the whistleblower. If the appropriate follow-up measures have not been determined after this period of time, the whistleblower should be informed about when feedback could be expected.
2. Feedback means that the whistleblower must be informed of what measures the Organization has taken or has intended to take, including the reasoning behind the chosen follow-up measures.

*Section 10*

**Record Keeping of Reports**

1. In compliance with the confidentiality requirements provided for in the national act implementing the Whistleblower Directive, Compliance Partners keep records of every report received. Reports are kept on the online platform. Reports shall be stored for no longer than it is necessary and proportionate, including in accordance with Compliance Partners’ time limits for the erasure of personal data.

*Section 11*

**Procedures for Reporting Externally**

1. The Organization is responsible for providing clear and easily accessible information to whistleblowers, about the procedures for reporting externally to competent authorities and, where relevant, to institutions, bodies, offices, or agencies of the EU. The Organization has, in addition to the below, provided this information in accordance with Section 1(5).
2. Whistleblowers can report externally to the following authorities:
	1. At the Danish Business Authority breaches, etc., can be reported relating to the area of accounting. More information regarding this external reporting channel can be found here: <https://erhvervsstyrelsen.dk/whistleblowerordning>.
3. Whistleblowers have freedom of choice regarding whether to report internally or externally.
1. Article 7. Directive (EU) 2019/1937 of the European Parliament and the Council of 23-10-2019, on the protection of persons who report breaches of EU law. [Link](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1937&qid=1691498171593). [↑](#footnote-ref-1)