Whistleblowing Policy

Status:	Released
Owner:	Anna Kołodziejczyk
Approved by:	Konrad Weiske
Authors:	Piotr Bączyk
Version:	1.0
Confidentiality:	*Public*
Released on:	2024-08-02

Revision history				
Version	Status	Date	Name	List of changes
0.0	Draft version	April 2024		
0.1	Released	April 2024	Anna Kołodziejczyk	
			Piotr Wierzba	
			Piotr Anioła	
			Jarosław Mroczek	
			Cezary Kożon	
			Sławomir Piwko	
			Michał Gronowski	
			Sławomir Podolski	
			Adam Pietraszek	
			Witold Leder	
			Remigiusz Morawiecki	
			Bartłomiej Lozia	
			Emilia Sękowska	
			Przemysław Ziemczyk	
			Duncan Johnson	
			Andrew Radcliffe	
			Igor Korzinek	
			Raul Halmagean	
			Ulf Magnus Wolkersdorfer	
			Konrad Weiske	
			Sebastian Łękawa	
			Wojciech Bodnaruś	
1.0	Released	August 2024	Piotr Bączyk	1. Removal of labour law related coverage from the basic Policy context and implementation of related changes; 2. Appendix 2 updates – Controllers full list, DPiA amendments; 3. Minor changes and wording adjustments; 4. Revision due to the current legislative status.

Table of Contents

Disclaimer

This Policy reflects a unified approach and the maintenance of identical and fair rules for everyone across the Spyrosoft Group, reflecting the rules and obligations imposed by Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of whistleblowers (the so-called Whistleblower Protection Directive) and those adopted in the various national legislations . However, it should be noted and emphasized that the national implementation of the Directive can and does take place differently in the individual EU States, and outside the EU is governed by separate laws. Therefore, the application of the Policy may differ slightly in each country in which the Spyrosoft Group operates. Therefore, the different elements specific to each country will be precisely indicated here, and their application, beyond the general provisions of the Policy, will be determined by Appendix 1, in which the specific additional provisions for each of the relevant countries can be found. What is more, there may be instances where this Policy, due to the variance with the local laws of a particular country may indicate different standards than the local law. Where local law imposes specific standards stricter than those set out in the present guidelines, local law will apply. If, by contrast, the present guidelines provide for a higher standard, it will prevail unless this results in illegal activity.

1. Introduction

Spyrosoft Group (Spyrosoft, Company) and all its subsidiaries are committed to conducting business according to legal, ethical, and social standards without corruption or conflict of interest. They also aim to eliminate all forms of discrimination, harassment, or compulsory labour and ensure that slavery and human trafficking do not occur in any part of the business or supply chain.

An important aspect of accountability and transparency is a mechanism to enable staff and other members of the Company, as well as authorized third parties (collectively referred to as individuals), to voice concerns responsibly and effectively. This policy applies to all individuals, especially – **employees** (understood as employees under labour law and all Spyrosoft collaborators working on the basis of b2b contracts, contracts of mandate and any other type of civil law contracts) in all companies within the Spyrosoft Group ("Spyrosoft") regardless of position held, seniority, or country.

We want to emphasize that this policy is intended to assist individuals who believe they have discovered malpractice or impropriety. It is not designed to question financial, or business decisions taken by the Company, nor should it be used to reconsider any matters which have already been addressed. This policy covers all cases of infringement by unlawful act or omission or intended to circumvent the law concerning [1]:

1. **human and civil liberties and rights** (to the extent not related to the other points, including, inter alia, violations of fundamental human rights, restriction of his/her freedom and liberty);
2. **corruption** (understood to be, for example, bribery and any form of monetary gain through position or contacts);
3. **public procurement** (concerns, inter alia, any irregularities occurring in public tenders);
4. **financial services, products, and markets** (concern, inter alia, all irregularities related to financial flows and financial operations related to financial products and services);
5. **anti-money laundering and countering the financing of terrorism** (include, inter alia, any behaviour or suspected breaches in this context);
6. **product safety and compliance** (e.g. with regard to circumventing certification obligations or otherwise failing to meet standards in production);
7. **transport safety** (inter alia, any behaviour or activity that can be assessed as objectively dangerous during and in connection with transport);
8. **environmental protection** (including, but not limited to, any conduct or activity that compromises safety or is contrary to applicable environmental regulations);

[1] The coverage legal provisions, which infringement by unlawful act or omission or intended to circumvent the law could be signaled under this policy, can be different in particular countries. Please find the differences in country specific Appendix 1.

9. **radiological protection and nuclear safety** (inter alia, any behaviour or activity that may cause a radiological emergency or violate nuclear safety procedures);
10. **food and feed safety** (inter alia, any infringement in the production, transport, storage and marketing of food);
11. **animal health and welfare** (including, but not limited to, acts that are unlawful or harmful to animals, and mistreatment of animals);
12. **public health** (inter alia, any negligence in the work context that may have negative consequences for the health of the individual);
13. **consumer protection** (inter alia, any act or failure to act in the context of service and consumer rights);
14. **protection of privacy and personal data** (including breaches of security rules and disclosure of confidential information to unauthorized persons);
15. **security of information and communication networks and systems** (including, but not limited to, improper storage of data, disclosure of passwords and facilitating unauthorized access to data by third parties);
16. **financial interests of the State Treasury, local self-government unit and the European Union** (inter alia, any infringement that may lead to the depletion of the assets of governmental and local institutions);
17. **the internal market of the European Union, including public competition law and state aid rules and corporate taxation** (inter alia, breaches of competition law through any form of unfair competition; use of unauthorized tax schemes and their improper accounting).

This Policy establishes the standards and procedures for reporting allegations, investigating, resolving problems, and preventing further violations in Spyrosoft. It also aims to provide a framework to promote responsible and secure SpeakUp by individuals without fear of adverse consequences and with a guaranteed level of confidentiality in the process.

The aims of this Policy are:

- To encourage individuals to report suspected wrongdoing as soon as possible, knowing that their allegations will be taken seriously and that appropriate investigation will take place.
- To provide individuals with guidance as to how to raise allegations, offering the possibility to report allegations through different levels of confidentiality (depending on the local regulatory environments).
- to reassure individuals that they should be able to raise genuine allegations without fear of retaliation and with safeguarding of their interests, even if they turn out to be mistaken.
- to implement at Spyrosoft an internal whistleblowing system that is uniform and fair for the entire group.

2. General Principles

Whistleblowing is a global grievance mechanism that allows the disclosure of information that relates to suspected wrongdoing, omissions, dangers at work, or indicated internal policy violations.

A whistleblower is a person who raises a justified allegation of wrongdoing or omission regarding infringement information obtained in a work-related context, following the process defined by this Policy and qualifies for whistleblower legal protections.

Everyone should be watchful for illegal, unsuitable, or unethical conduct and report anything of that nature that they become aware of. Speak-up; if you see something - say something!

Disclosure of the acts of wrongdoing or omission, if properly made (i.e., in good faith and without personal gain), carries full protection within the law, subjected to any other detriment, or discrimination because of the disclosure. We guarantee that no disciplinary measures or other steps will be taken against you if your genuine concern later turns out to be mistaken or misguided.

The whistleblower should never investigate the matter himself/herself nor seek evidence to build a strong case. Moreover, simultaneously recommending the use of internal channels under the Policy in the first place, we indicate that the whistleblower can in any case easily and in an accessible way make external reports (inter alia to Ombudsmen or other locally designated entities), which have been specified and to which we refer in the national Appendixes.

3. Safeguards

1. Protection

A whistleblower is considered to act “in good faith” when he/she provides information that he/she believes is comprehensive, fair, and accurate and has legitimate grounds for doing so, even if it later appears that he/she was mistaken. The whistleblower is protected from the moment the notification is made in accordance with this procedure. In addition, we point out that every whistleblower is also entitled to additional support resources in the form of the possibility to make use of national systems of free legal and civic support as far as the role of the whistleblower is concerned.

2. Confidentiality

Spyrosoft will treat all such disclosures in a confidential and sensitive manner. The identity of the individual making the allegation may be kept confidential so long as it does not hinder or frustrate any investigation. However, the investigation process may reveal the source of the information, and the individual making the disclosure may need to provide a statement as part

of the required evidence. Throughout and after the proceedings, the whistleblower will be afforded special regulatory protection in relation to the notification made and its repercussions.

The procedure also provides for the possibility of anonymous reporting; however, this involves certain formal restrictions.

3. Anonymous Submissions [2]

This policy encourages individuals to put their names on any disclosures they make. Concerns expressed anonymously are much less credible and harder to prove but will be considered with the same seriousness, inquisitiveness, and due consideration as applications under the normal procedure. On the other hand, it should be borne in mind that, at a certain stage of the proceedings, proof of wrongdoing or negligence may require a certain degree of disclosure or identification during the process of the whistleblower - in such a case, Spyrosoft is bound by the previously indicated standards of confidentiality. At any stage, a whistleblower may decide to disclose their data - particularly if it may assist the investigation.

4. Untrue Allegations [3]

If an individual makes an allegation in good faith, on reasonable grounds, which are not confirmed by subsequent investigation, no action will be taken against that individual. In disclosing, the individual should exercise due care to ensure the information's accuracy. If, however, an individual makes malicious or vexatious allegations, and particularly if he or she persists in making them, disciplinary action may be taken against that individual as well as bear the liability for damages prescribed by law and may also involve appropriately regulated criminal liability in the most serious cases.

5. Principle “no one shall be a judge in his own cause”

This principle is a fundamental legal principle and shall apply here. We believe that a fair and impartial decision can only be reached if the decision-maker is impartial and unbiased. Therefore:

- An appointed investigator can voluntarily step out or not be involved in the entire process if he/she deems that a concern creates a conflict of interest. Whenever a whistleblower doubts whether a particular investigator can participate in proceedings, the Case Unit Review will examine the possibility of participation and rule on its possible exclusion from such proceedings.

[2] Anonymous submissions allowance could be interpreted / implemented different in particular countries. Please find the differences in country specific Appendix 1.
[3] The consequences of Untrue Allegations can differ in particular countries. Please find the differences in country specific Appendix 1.

- Complaints against the Whistleblowing Officer, Whistleblowing Champion or any Case Unit Review member will be considered by a Committee of Case Unit Review's other independent members supervised by a designated whistleblower Board Member of the Group.

6. Local reconnaissance

Taking into account the group nature of the application of the Policy, Spyrosoft, at the same time, ensures that the case of each whistleblower will be - depending on the nature and scope of the case - as far as possible investigated locally, i.e., at the place of work/cooperation/report of a given whistleblower.

4. Raising an allegation

We want all individuals to be able to raise any allegations at any stage with the Whistleblowing Officer and / or Whistleblowing Champion.

Hereby, we present the Policy structure for raising allegations and responsible officers:

1. The Whistleblowing Officer has the responsibility to ensure that this Policy is operated correctly so that individuals can raise allegations without fear of retaliation and ensure that the provisions of the procedure are implemented in a timely and compliant manner. The Whistleblowing Officer is also responsible for addressing concerns and questions of individuals regarding ethics or wrongdoing/ omissions and assisting with investigations and resolutions of ethics/ omissions issues.

2. The Whistleblowing Champion supports the Whistleblowing Officer's activities and performs its duties at the individual company level with additional, organisation-specific expertise.

3. Case Unit Review—Within Spyrosoft Group, it has been decided that the investigations will be led by the Case Unit Review, consisting of three members: a Whistleblowing Officer, a Whistleblowing Champion (dedicated to a particular company), and a designated lawyer. From time to time, and depending on the circumstances, members can differ (a local representative or domain expert / relevant employee may be added/required to join the investigation). The investigation is supervised by a designated whistleblower Board Member of the Group.

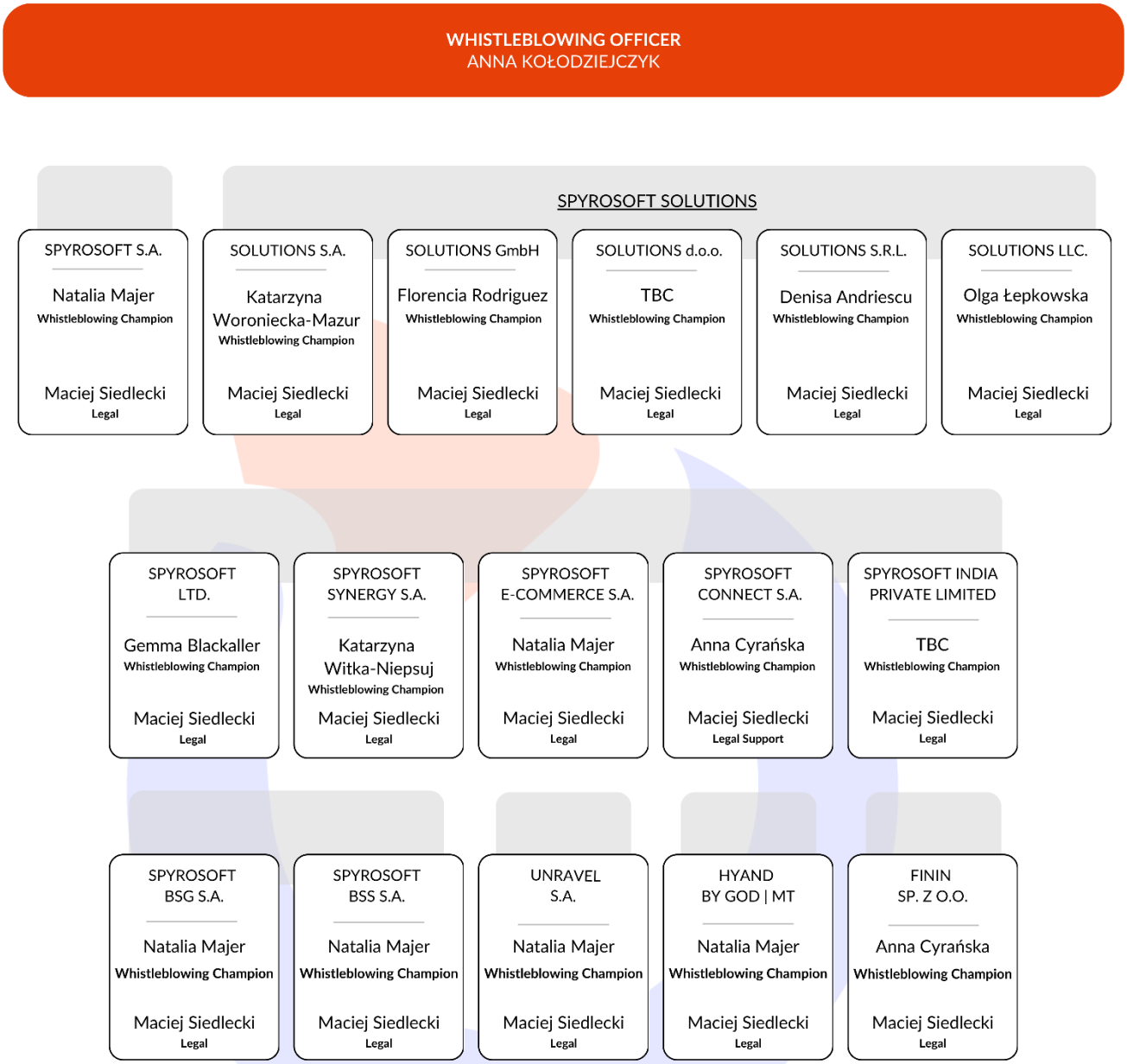
4. Designated whistleblower Board Member of the Group—is the body that supervises the regularity of the policy proceedings, is the appeal body against the Case Unit Review's report, and issues the final ruling on a particular case within the framework of the evidence collected.

You can raise the allegation [4]:

[4] The possibilities of raising an allegation can differ in particular countries. Please find the differences in country specific Appendix 1.

- via email to SpeakUp@spyro-soft.com, having in mind that:
  - confidentially, using the e-mail address within the Spyrosoft domain or within the external domain, but including your name and surname – you accept the right to be contacted by the investigator; you will be informed, when possible, of the overall findings. Please note that it is possible that we will not be able to give you full details of the outcome of a case (or related actions taken) for reasons of confidentiality, privacy, and the legal rights of all concerned;
  - anonymously, using the external e-mail address with a nickname that cannot be associated with you; in this case, the investigator will be able to communicate with you only by this channel; however, the exchange will be limited in this capacity.
- In writing as a formal letter -> with the indication "Confidential, to be passed over to the Whistleblowing Officer,"
- By arranging an appropriate call within available slots with the Whistleblowing Officer (no later than 14 days from the date of notification) or by recording a message and sending it via available channels to the Whistleblowing Officer,
- Directly to the Whistleblowing Officer, by any possible means.

Case Unit Review



5. Timescales[5]

Due to the varied nature of these sorts of complaints, which may involve internal investigators and/or the police, Appendix 1 indicates only framework deadlines for the investigation outcome of each whistle-blown. The Case Unit Review will ensure the case is undertaken as quickly as possible, with follow-up actions planned and implemented, considering the obligation to follow the country-specific timeframe.

[5] The timescales of the procedures are individual in particular countries. Please find the differences in country specific Appendix 1.

The Case Unit Review should, as soon as practically possible, form their appropriate composition and send a written acknowledgment of the concern to the complainant and thereafter report back to them in writing the outcome of the investigation, which is consulted by a designated whistleblower Board Member of the Group. If the investigation is a prolonged one, the Case Unit Review should keep the complainant informed, in writing, as to the progress of the investigation and as to when it is likely to be concluded.

All communication should be in writing, following the channels and e-mail address used for raising the allegations.

6. Investigation and outcome

Once an allegation is raised, it will be thoroughly investigated with due professional diligence. The whistleblower will receive an e-mail acknowledgment that the information has been received and the case has been registered. The whistleblower may be required to provide additional information. Once completed, the whistleblower will be informed of the outcome of the pending proceedings insofar as this is possible in the context of the decision taken.

Investigations will be conducted in an independent, fair and unbiased manner with respect to all parties involved and in accordance with relevant laws and principles (including fair hearing), by the Case Unit Review. The Case Unit Review's members will be adequately trained for their roles - Spyrosoft will prepare in a structured and detailed manner and ensure that the level of knowledge, familiarity with Procedure and regulations is regularly consolidated, and that an appropriate level of confidentiality is maintained among the team, providing the quality and tools to do so.

Details of the case, the whistleblower's identity (if known) and the identity of anyone else mentioned in the report, in accordance with the principles for processing those data, are kept confidential throughout and after the investigation and are only shared on a need-to-know-statutory-basis.

If the whistleblower becomes involved in an investigation, he/she needs to cooperate and answer all questions completely and honestly to the best of their knowledge. Misrepresenting or declaring false information to the investigators of the whistleblower's case and interfering with an ongoing investigation may lead to disciplinary (employees only), compensation and criminal measures.

All parties involved, including the accused, are entitled to confidentiality to avoid unnecessary reputational damage. Therefore, if the whistleblower participates in or learns about an investigation, he/she must keep the matter confidential.

We will deal with allegations fairly and appropriately, using this Policy and the investigation best practices to help us achieve this. Thus, individuals may see changes in day-to-day activity regarding the allegations raised.

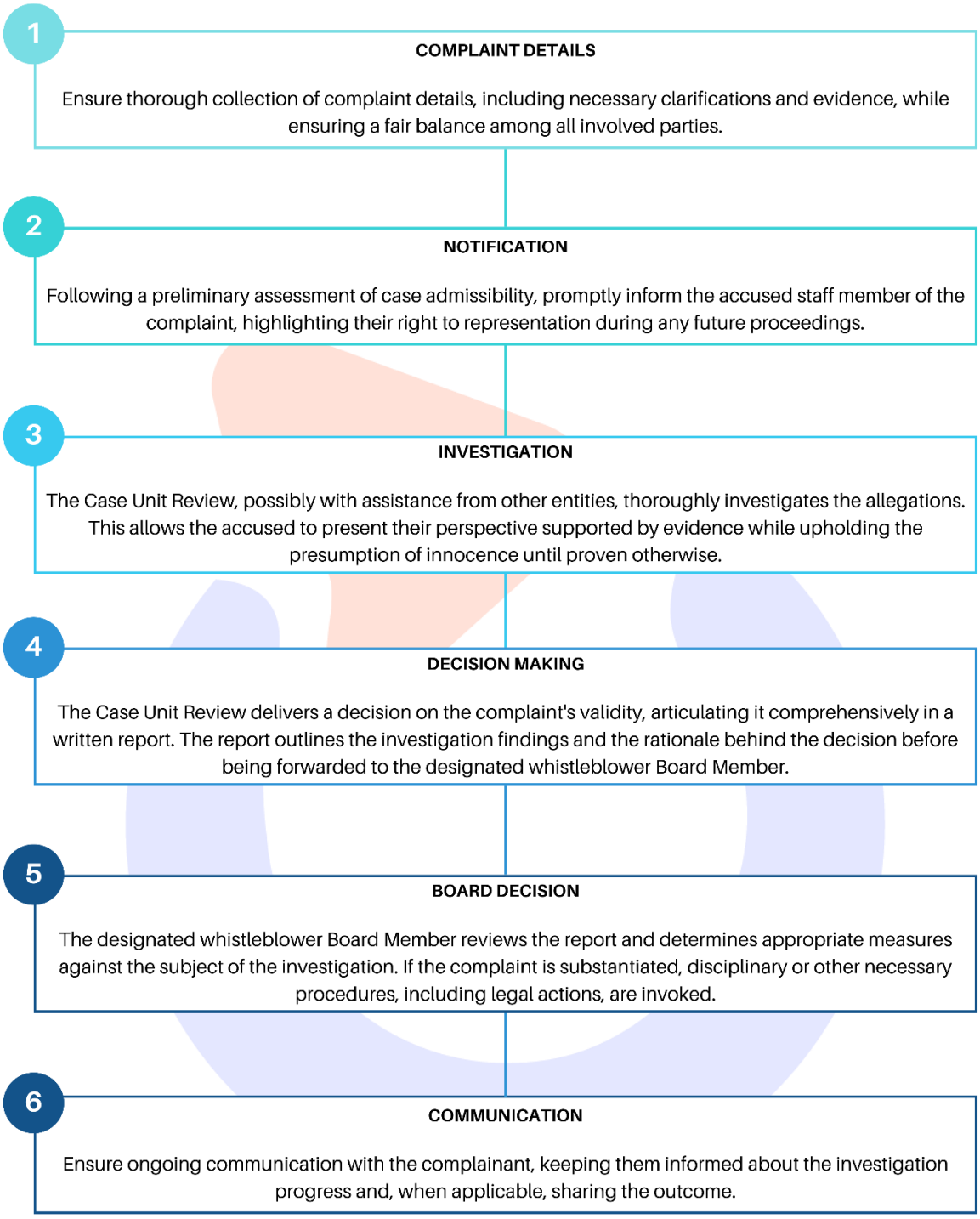
However, if you see further evidence that the wrongdoing is continuing, the whistleblower should contact the Whistleblowing Officer.

The Case Unit Review should follow these steps:

- Full details and clarifications of the complaint should be obtained within the complete evidence while maintaining a balance between the interested parties.
- The Case Unit Review, after a preliminary examination of the case's admissibility, should inform the individual against whom the complaint is made as soon as practicable. The individual will be informed of their right to be accompanied by any representative at any future interview or hearing held under the provisions of these procedures.
- The allegations should be fully investigated by the Case Unit Review with the assistance, where appropriate, of other individuals/bodies, on a confidential basis. This would allow the accused party to present its position supported by the evidence presented and to remain neutral as an innocent person until proven otherwise.
- The Case Unit Review will decide the complaint's validity. This decision will be articulated in a comprehensive written report outlining the investigation findings and rationale behind the decision. Subsequently, the report will be forwarded to the designated whistleblower Board Member of the Group as deemed appropriate.
- The designated whistleblower Board Member of the Group rules on the measures to be taken against the subject of the investigation as part of a decision reported by Case Unit Review—it is made after the report is delivered to the whistleblower and other Parties. If the complaint is shown to be justified, then they will invoke disciplinary or other appropriate procedures (including civil/criminal path).
- The whistleblower should be kept informed of the progress of the investigations and, if appropriate, of the outcome.

If the whistleblower is not satisfied that the Case Unit Review officer is properly handling their concern, they have the right to raise it in confidence with the designated whistleblower Board Member of the Group, who is the appeal authority against the report of the Case Unit Review.

This is the final step, and decisions made here are final, with no further options for appeal. However, the above does not exclude the individuals' right to use other available legal means, including the right to file an appropriate claim within the institutions appointed in particular countries (as specified in Appendix 1).



7. Protection and support

We understand that people who raise allegations at work are sometimes worried about possible repercussions or retaliation. We encourage openness and will support individuals who raise genuine allegations in the common interest under this Policy, even if they are mistaken.

Individuals will not suffer any detrimental treatment as a result of raising allegations provided they reasonably believe and have justified grounds that the allegations are true, that the disclosure is being made to the correct person/body, and that the allegations are not made for personal gain.

"Detrimental treatment[6]" might include, among others, dismissal, disciplinary action, bullying, discrimination, or threats. Any individual who believes that they have suffered such treatment should inform the Whistleblowing Officer immediately, who will initiate a check and will prevent this type of action, providing the individual with the protection envisaged.

Spyrosoft and other individuals must not threaten, bully, harass, or retaliate against whistleblowers, and anyone who is involved in such conduct will be subject to disciplinary (employees only) and criminal actions which may lead to dismissal, punishable by a fine and, in the most extreme cases, by imprisonment.

Please remember that any person who speaks up is protected. Please feel confident that you will not suffer for raising concerns in good faith about suspected misconduct or omission.

This Policy does not guarantee protection from disciplinary action where the individuals who have raised the allegation are found to have committed the wrongdoing themselves. However, their raising of an issue may be considered a significant mitigating factor in any possible disciplinary or criminal proceedings.

Any reports made through this Policy that are found to have been raised maliciously or in the knowledge that they were untrue may result in disciplinary, compensation, and even criminal actions being taken against the individuals.

Disciplinary actions[7] may include but are not limited to, verbal or written warnings, suspension from work/provision of services, demotion, loss of privileges, mandatory training, or termination of cooperation, irrespective of the form of the contract (employees only). The decision on the appropriate disciplinary action will be made at the company's discretion, based on the constructed report, considering the nature and impact of the policy violation.

8. Data protection, data storage and information security

Your information is safe with us, and the data and details of individual cases are stored and protected appropriately - only available to a specific audience and used during an investigation on a statutory "need to know" basis.

[6] May be interpreted differently in particular countries.
[7] May be interpreted differently in particular countries.

The details of data protection, data storage, and information security in the scope of inter alia: the administrator, the method of storage, the duration of storage, your rights and the security of the information, the safeguards applied, and any necessary reservations in this respect were regulated and presented in Appendix 2.

For any further information in this matter, please contact the Whistleblowing Officer or Data Protection and Information Security Officer indicated therein.

9. Key contacts and policy ownership

Spyrosoft will review the policy at least every 2 years to identify any weaknesses and make changes to maintain compliance with applicable laws and regulations or accommodate organizational changes within Spyrosoft.

Further information, queries, or comments about this policy should be addressed to the Whistleblowing Officer.

Role	Name	Contact details
Whistleblowing Officer	Anna Kołodziejczyk	SpeakUp@spyro-soft.com
Whistleblowing Champions **1. Spyrosoft S.A.** **2. Spyrosoft Solutions S.A.** **3. Spyrosoft Solutions GmbH** **4. Spyrosoft Solutions d.o.o.** **5. Spyrosoft Solutions S.R.L** **6. Spyrosoft Solutions LLC** **7. Spyrosoft Ltd.** **8. Spyrosoft Synergy S.A.** **9. Spyrosoft eCommerce S.A.** **10. Spyrosoft Connect S.A.** **11. Spyrosoft India Private Limited** **12. Spyrosoft BSS S.A.** **13. Spyrosoft BSG S.A.** **14. Hyand by GOD | MT** **15. Unravel S.A.** **16. Finin Sp. z o.o.**	1. Natalia Majer 2. Katarzyna Woroniecka-Mazur 3. Florencia Rodriguez 4. TBC 5. Denisa Andriescu 6. Olga Łepkowska 7. Gemma Blackaller 8. Katarzyna Witka-Niepsuj 9. Natalia Majer 10. Anna Cyrańska 11. TBC 12. Natalia Majer 13. Natalia Majer 14. Natalia Majer 15. Natalia Majer 16. Anna Cyrańska	SpeakUp@spyro-soft.com
Legal whistleblowing support	Maciej Siedlecki	SpeakUp@spyro-soft.com

Designated whistleblowing Board Member of the Group	Wojciech Bodnaruś	SpeakUp@spyro-soft.com

Appendix 1.1 – Poland

This Annex indicates the individual provisions, conditions, and rules of the Policy specific to the country indicated in the title of the Annex. Please note that in the event of any dispute or inconsistency with national regulations, the provisions of the national regulations take precedence over those of the Policy.

Timeline overview

This Policy and its Appendix 1.1 will be circulated for consultation with employees. They can submit their comments within 10 days of the announcement of the procedure's content being implemented. After reviewing the comments, Spyrosoft will announce the procedure's final form.

Procedure and Timeliness	Deadline
Deadline for acknowledgment of receipt of the submission	**Immediately**, automatically, or on the day of receipt
Deadline for acknowledgment of acceptance for processing or rejection/request for completion	**7 days** from receipt of application
Deadline for feedback and follow-up	Maximum **3 months** from the date of submission, with a **possible extension to 6 months** if necessary. Reasons for extension must be documented and communicated.
Finalization of investigation and report	Report to be forwarded within **7 days** of completion of the investigation
Final decision on next steps and resolution	Within **7 days** of receiving the report, the Relevant Board Member designated for whistleblowers makes final decisions based on its recommendations and conclusions.

1. **Provisions on the processing of personal data**:

1.1. Once a submission has been received, the personal data received is processed to the extent necessary for its acceptance or follow-up. Personal data that is not relevant for the processing of the request shall not be collected and, if accidentally collected, shall be deleted immediately. The deletion of personal data shall take place within **14 days** of the determination that it is not relevant.

1.2. Personal data processed in connection with the acceptance of a submission or follow-up and documents relating to that submission shall be retained for a period of **3 years** after the end of the calendar year in which the notification was transmitted to the authority competent to take follow-up action, the follow-up action was completed, or the proceedings initiated by those actions are concluded.

2. Procedure and timeliness of the handling of the submission:

2.1. Deadline for acknowledgment of receipt of the submission - **immediately**, automatically or, in case of other available channels, on the day of receipt of the submission;
2.2. Deadline for acknowledgment of acceptance for processing (or rejection if there are insufficient grounds) / request for completion - **7 days** from receipt of application;
2.3. The deadline for feedback and follow-up is a maximum of 3 months from the date of receipt of the submission. If necessary, this time limit may be extended to 6 months if the circumstances of the case and the nature of the problem reported require a longer procedure. In this case, the reasons for the extension should be properly documented and communicated to those concerned.
2.4. The investigation should be finalized with a report, including recommendations for a decision on the pending submission. The report shall be forwarded within **7 days** of its completion to the parties concerned and to the relevant board Member designated for whistleblowers. The Relevant Board Member designated for whistleblowers shall, within 7 days after receipt of the report regarding its recommendations and bound by its conclusions, make the final decisions on the next steps and resolution of the case.

3. Personal scope of whistleblower protection:

Within the meaning of Polish regulations, a whistleblower may be a person making an internal report within the framework of the Policy, in good faith, in a context related to the work performed, among others:
3.1. employed under a contract of employment (irrespective of its duration and type);
3.2. Cooperating based on a contract of mandate, contract for specific work, management contract, contract for the provision of services (b2b contract);
3.3. Partner, shareholder, funder;
3.4. Member of the Board;
3.5. Member of the Supervisory Board, audit committee, proxy;
3.6. Volunteer, trainee, apprentice.

4. Liability for false reporting (bad faith) and liability in a whistleblower protection system

4.1. In addition to disciplinary and compensatory liability, national legislation provides for criminal liability for several irregularities related to the provisions of the Policy - this is regulated in detail by the provisions of Chapter 6 of the Whistleblowers Act. Criminal liability will be incurred by:
4.1.1. Individuals preventing/obstructing notification;
4.1.2. Taking retaliatory action against a whistleblower, an individual assisting in making a report or associated with a whistleblower;
4.1.3. Disclosing the identity of the whistleblower, the person assisting in making the report or associated with the whistleblower;
4.1.4. Submitting a report or making a public disclosure with the knowledge that no infringement has occurred.

5. Supporting institution and contact details

5.1 National implementation of the obligations arising from the Directive - the Act on whistleblowers entrusts the tasks of the institution supporting whistleblowers to the Ombudsman. This body is established to protect the rights of citizens, and its independence and independence is guaranteed by the Constitution of the Republic of Poland. Everyone has the right to apply, on the principles set out in the Act, to the Ombudsman for assistance in protecting his or her freedoms or rights violated by public authorities, and the Ombudsman himself or herself upholds the freedoms and rights of human beings and citizens set out in the Constitution and other normative acts, including the implementation of the principle of equal treatment.

In implementing the provisions of the Act, the Ombudsman will be both the body authorized to provide information and support to whistleblowers and responsible for receiving so-called external notifications. The institution to which the Ombudsman will forward the notification will be obliged to provide feedback to the notifier, to take follow-up actions and to provide the Ombudsman with comprehensive information on the actions taken regarding the notification.

You can contact the Ombudsman via:
- website: https://bip.brpo.gov.pl/pl/content/zlozenie-wniosku-do-rzecznika-praw-obywatelskich using the online form;
- ePUAP mailbox: https://epuap.gov.pl/wps/myportal/aplikacje/skrzynka?formSubId=RPO&serviceId=SC:51168&formName=UGlzbW8gb2fDs2xuZSB6IG9ic8WCdWfEhSBkdcW8eWNoIHBsaWvDs3c=&kupName=UGlzbW8gb2fDs2xuZSBkbyBSemVjem5pa2EgUHJhdyBPYnl3YXRlbHNraWNo;
- e-mail address: biurorzecznika@brpo.gov.pl;
- in writing to: Biuro Rzecznika Praw Obywatelskich, al. Solidarności 77, 00-090 Warszawa;
- in person during duty hours at the Ombudsman offices in Warsaw, Katowice, Gdańsk or Wrocław, or during duty hours in the cities indicated on the website.

You can also obtain any additional information from the Ombudsman Office hotline on the following telephone numbers: 800 676 676 and (22) 551 77 91.

5.2 In addition, whistleblowers are also entitled to report through external channels (bypassing the internal procedure), including to other relevant authorities that may have jurisdiction over the type of case in question.

Appendix 1.2 - Romania

This Annex indicates the individual provisions, conditions, and rules of the Policy specific to the country indicated in the title of the Annex. Please note that in the event of any dispute or inconsistency with national regulations, the provisions of the national regulations take precedence over those of the Policy.

Timeline overview

Procedure and Timeliness	Deadline
Deadline for acknowledgment of receipt of the submission	**Immediately**, automatically, or on the day of receipt
Deadline for acknowledgment of acceptance for processing or rejection/request for completion	**7 days** from receipt of application
Deadline for feedback and follow-up	Maximum **3 months** from the date of submission, with a **possible extension to 6 months** if necessary. Reasons for extension must be documented and communicated.
Finalization of investigation and report	Report to be forwarded within **7 days** of completion of the investigation
Final decision on next steps and resolution	Within **7 days** of receiving the report, the Relevant Board Member designated for whistleblowers makes final decisions based on its recommendations and conclusions.

1. Provisions on the processing of personal data and confidentiality of the data

1.1 Legal entities shall keep a record of all reports received, subject to confidentiality requirements. Reports shall be kept for **5 years**, after which they will be destroyed.

1.2 Information in the reports that constitutes trade secrets may not be used or disclosed for purposes other than those necessary to resolve the report.

2. Procedure and timeliness of the handling of the submission:

2.1 Deadline for acknowledgment of receipt of the submission - **immediately**, automatically, or, in case of other available channels, on the day of receipt of the submission;

2.2 Deadline for acknowledgment of acceptance for processing (or rejection if there are insufficient grounds) / request for completion - **7 days** from receipt of application;

2.3 Deadline for feedback and follow-up - maximum **3 months** from the date of receipt of the submission. This time limit may be extended to **6 months**, if necessary if the circumstances of the case and the nature of the problem reported requiring a longer procedure, in which case the reasons for the extension should be properly documented and communicated to those concerned.

2.4 The investigation should be finalized with a report, including recommendations for a decision on the pending submission. The report shall be forwarded within **7 days** of its completion to the parties concerned and to the relevant board Member designated for whistleblowers. The Relevant Board Member designated for whistleblowers shall, within 7 days after receipt of the report regarding its recommendations and bound by its conclusions, make the final decisions on the next steps and resolution of the case.

3. Personal scope of whistleblower protection

The Whistleblowing Law protects and encourages the act of whistleblowing and also applies to persons whose employment relationship has not yet begun and who make reports through internal or external reporting channels or publicly disclose information on violations of the law obtained during the recruitment process or other pre-contractual negotiations, or when the employment or service relationship has ended.

4. Liability for false reporting (bad faith) and liability in a whistleblower protection system

4.1 The following act (Law No 361/2022 on the protection of whistleblowers in the public interest) constitutes contraventions, if they have not been committed under such conditions as to be considered, according to the criminal law, offenses and shall be sanctioned as follows:

4.2 the prevention, by any means, of reporting by the person designated to receive and record the reports or by the person who is part of the department designated for this purpose within private and public legal entities with a fine ranging from 2,000 lei to 20,000 lei;

4.3 unjustified refusal to respond to the requests of the authorities in the exercise of their duties, with a fine of 3,000 lei to 30,000 lei;

4.4 reporting information on violations of the law knowing it to be untrue, with a fine of 2,500 lei to 30,000 lei.

5. Additional measures and supporting institutions:

5.1 As part of the national procedure in Romania, Spyrosoft also covers violations arising from labour law in its broadest sense and the whistleblower protection associated with reporting them - under Procedure.

5.2 An effective measure to support whistleblowers in challenging any form of retaliation is the provision of free legal assistance by the Bar Association upon the whistleblower's request—we encourage you to seek help from your local lawyers during the process.

5.3 Additionally, you can also report infringements online via the Romanian Integrity Agency (*Agentia Nationala de Integritate*), where a general external reporting system has been launched and can be accessed online at https://avertizori.integritate.eu/.

Appendix 1.3 - United Kingdom

This Annex indicates the individual provisions, conditions, and rules of the Policy specific to the country indicated in the title of the Annex. Please note that in the event of any dispute or inconsistency with national regulations, the provisions of the national regulations take precedence over the provisions of the Policy.

Timeline overview

Procedure and Timeliness	Deadline
Deadline for acknowledgment of receipt of the submission	**Immediately**, automatically, or on the day of receipt
Deadline for acknowledgment of acceptance for processing or rejection/request for completion	**7 days** from receipt of application
Deadline for feedback and follow-up	Maximum **3 months** from the date of submission, with a **possible extension to 6 months** if necessary. Reasons for extension must be documented and communicated.
Finalization of investigation and report	Report to be forwarded within **7 days** of completion of the investigation
Final decision on next steps and resolution	Within **7 days** of receiving the report, the Relevant Board Member designated for whistleblowers makes final decisions based on its recommendations and conclusions.

Due to Brexit, the UK is not a member state of the EU, but some of the connecting legal obligations continue to exist. Unfortunately, the Whistleblowing Directive is not one of them. The UK had its regulations in place much earlier, and they are the main basis for enforcement and policy implementation in the country today.

For this reason, in the UK, the Policy's legality will first be determined by locally adopted laws that regulate the content and values covered.

However, UK legislation includes both a definition of a whistleblower and the scope of their responsibilities, which are far narrower than the Directive and the Policy adopted by Spyrosoft. With this in mind, Spyrosoft ensures equal and fair treatment of all collaborators in the group, guaranteeing the same quality and regulations worldwide, regardless of country.

The Policy as introduced will, therefore, be in full force and effect, except for elements that could be considered contrary to the regulations - in which case the provisions of United Kingdom law apply.

1. **The UK fundamental legislation grounds for whistleblowing systems**:

    1.1. Employment Rights Act (1996);

1.2. Public Interest Disclosure Act (1998);

1.3. The grounds of protection are much more narrow then the EU ones. Whistleblower is protected when recognized as a worker (within the UK understanding) – an employee, a trainee, an agency worker, or a member of a Limited Liability Partnership (LLP). Also, the list of possible complaints is much shorter – it does not include, e.g., personal grievances unless the particular case is in the public interest.
If you are not sure whether your claim is valid – contact us; we assure you that we provide much more than proposed via internal whistleblowing channels.

1.4. While there is no general obligation on workers to disclose wrongdoing, certain categories of employees – particularly those in the regulated sector – may have specific reporting obligations to their employers or regulators. The Employment Rights Act 1996 (ERA), as amended by the Public Interest Disclosure Act 1998 (PIDA), provides protection to workers who blow the whistle by protecting them against detrimental treatment and (in the case of employees) from being dismissed for making certain specified types of 'qualifying protected disclosures'. Compensation for successful Employment Tribunal whistleblowing claims is uncapped. Such legal protections relate only to dismissal or detriment in an employment context and do not provide immunity from criminal prosecution where a whistleblower is implicated in criminal conduct.

1.5. Outside the financial services sector, there is currently no requirement for organizations in the United Kingdom to have whistleblowing mechanisms. However, the EU Directive on the protection of persons reporting on breaches of Union law (the Whistleblower Directive) was formally adopted in October 2019. In addition, in July 2019 a report of the All Party Parliamentary Group (APPG) for Whistleblowing recommended the introduction of mandatory internal and external reporting mechanisms along with meaningful penalties for those who fail to meet the requirements across all sectors.
The APPG has also urged the government to ban the use of non-disclosure agreements (NDAs) in whistleblowing cases. The use of NDAs in settlements with employees has attracted considerable media attention in the wake of the #MeToo movement – such NDAs are unenforceable.

2. Additional procedures and timeliness of the handling of the submission:

2.1. Deadline for acknowledgment of receipt of the submission - **immediately**, automatically or, in case of other available channels, on the day of receipt of the submission;

2.2. Deadline for acknowledgment of acceptance for processing (or rejection if there are insufficient grounds) / request for completion - **7 days** from receipt of application;

2.3. Deadline for feedback and follow-up - maximum **3 months** from the date of receipt of the submission. This time limit may be extended to **6 months**, if necessary if the circumstances of the case and the nature of the problem reported requiring a longer procedure, in which case the reasons for the extension should be properly documented and communicated to those concerned.

2.4. The investigation should be finalized with a report, including recommendations for a decision on the pending submission. The report shall be forwarded within **7 days** of its completion to the parties concerned and to the relevant board Member designated for whistleblowers. The Relevant Board Member designated for whistleblowers shall, within 7 days after receipt of the

report regarding its recommendations and bound by its conclusions, make the final decisions on the next steps and resolution of the case.

2.5. Additionally, Spyrosoft while dealing with the submission will:

2.5.1. Record all of the numbers of whistleblowing disclosures that were received and register their nature;

2.5.2. Maintain records of the date and content of feedback provided to whistleblowers;

2.5.3. Conduct regular surveys to ascertain the satisfaction of whistleblowers.

2.6. If a whistleblower believes that they have been unfairly treated because they have blown the whistle they may decide to take their case to an employment tribunal. The process for this would involve attempted resolution through the Advisory, Conciliation and Arbitration Service (ACAS) early conciliation service.

3. Provisions on the processing of personal data:

3.1. Of course, across the EEA, organizations must comply with data protection requirements under the GDPR when processing personal information collected from whistleblowing hotlines. Similar rules apply in the UK under the UK GDPR. Common requirements include (*inter alia*):

3.1.1. Providing notice to employees about the organization's whistleblowing programme and data collection practices. This is usually satisfied by providing a privacy notice before or when the data is collected. It is best practice to implement a privacy notice specific to the hotline;

3.1.2. Keeping data for no longer than is necessary. There are no specific retention periods but the expectation is that the data is retained for as long as is needed to fulfill the organizations' collection purposes.

3.1.3. Complying with cross-border transfer restrictions. The GDPR and its UK equivalent only allow cross-border data transfers under limited circumstances, including where a country is recognized as providing adequate protection to the data, or where an authorized data transfer mechanism is used.

3.1.4. Registering data processing activities with local data protection authorities when required to do so legally. Specific registration requirements vary by jurisdiction and each data protection authority imposes its own formalities.

3.2. As Spyrosoft may engage third parties to operate a whistleblower hotline, it is important to include clauses in the contract with the third-party service provider that give employers adequate protection. Contracts should comply with Article 28 processor requirements, including by ensuring personal data is processed in line with the employer's instructions, the data is only used for specified purposes, and security measures have been implemented.

3.3. Any employee request to access, delete, or correct data collected from the hotline must also be acted on. Using defined retention periods and criteria for the personal data to be collected, encryption technology, and measures to ensure the reporter's anonymity are also essential—all relevant to the UK GDPR.

4. Special requirements resulting from the FCA:

4.1. A key component of the SMCR is a requirement for firms to appoint a whistleblowers' champion with responsibility for ensuring and overseeing the integrity, independence and

effectiveness of the firm's policies and procedures on whistleblowing. The FCA expects that this role will be filled by a non-executive director. Assignment of specific responsibility for whistleblowing to a senior person – preferably the chairman – was a recommendation of the June 2013 report of the Parliamentary Commission on Banking Standards, Changing Banking for Good, and is consistent with the broader trend towards senior management responsibility in the UK regulatory regime. This is reflected both in the fact that the whistleblowers' champion is now a prescribed responsibility under the SMCR, and in the guidance that the whistleblowers' champion should have a level of authority within the firm sufficient to carry out their function. **Such measures have been implemented in the Policy, where we proposed a hierarchical structure in terms of supervision and operation within the framework of proceedings from submissions.**

4.2. **The whistleblowers' champion is also expected to ensure that an annual report is presented to the board regarding the effectiveness of whistleblowing systems and controls.** The FCA and PRA have not been prescriptive about how whistle-blowers' champions perform their role, and have acknowledged that firms are likely to take different approaches depending on their structure and size. In smaller firms, the whistleblowers' champion may choose to take a 'hands-on' role, possibly in concert with his or her support staff, receiving disclosures personally and taking responsibility for disseminating reports within the firm, tracking progress, making external reports, feeding back to whistleblowers where appropriate and reviewing settlement agreements. In larger firms, whistleblowers' champions are more likely to perform their function by delegating day-to-day operations to a dedicated whistleblowing function while retaining an oversight role. The PRA expects the whistleblowers' champion to have access to resources and information sufficient to carry out their role. In practice, this is likely to include a regular suite of management information on the number and outcome of reportable concerns, as well as analysis or oversight of patterns in data – for example, particular business units or offices in respect of which reportable concerns are more frequently raised.

4.3. **As to the settlement agreements with workers** - the FCA's rules require a firm to include in a settlement agreement with a worker a term making clear that nothing in that settlement agreement prevents the worker from making a protected disclosure.

5. **Supporting institution and contact details**:

5.1. Contact the Advisory, Conciliation and Arbitration Service (ACAS) for help and advice on resolving a workplace dispute. You can find ACAS via https://www.acas.org.uk/advice.

5.2. If you decide to blow the whistle to a prescribed person rather than your employer, you must make sure that you have chosen the correct person or body for your issue. For example, if you are blowing the whistle on broadcasting malpractice you should contact the Office of Communications (Ofcom). At the attached link, you can find a list of the prescribed persons and bodies to whom you can make a disclosure. There is also a brief description of the matters you can report to each prescribed person: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies

6. **Labor law cases** - As part of the national procedure in United Kingdom, Spyrosoft also covers violations arising from labour law in its broadest sense and the whistleblower protection associated with reporting them - under Procedure.

Appendix 1.4 – Argentina

This Annex indicates the individual provisions, conditions, and rules of the Policy specific to the country indicated in the title of the Annex. Please note that Argentinian regulations have been analyzed for the overall purpose of this policy since Argentina is not a member of the EU; but due to contractual terms, Policy terms are conveyed under the Polish process for Argentina collaborators.

Timeline overview

This Policy and its Appendix 1.4 will be circulated for consultation with employees. They can submit their comments within 10 days of the announcement of the procedure's content being implemented. After reviewing the comments, Spyrosoft will announce the procedure's final form.

Procedure and Timeliness	Deadline
Deadline for acknowledgment of receipt of the submission	**Immediately**, automatically, or on the day of receipt
Deadline for acknowledgment of acceptance for processing or rejection/request for completion	**7 days** from receipt of application
Deadline for feedback and follow-up	Maximum **3 months** from the date of submission, with a **possible extension to 6 months** if necessary. Reasons for extension must be documented and communicated.
Finalization of investigation and report	Report to be forwarded within **7 days** of completion of the investigation
Final decision on next steps and resolution	Within **7 days** of receiving the report, the Relevant Board Member designated for whistleblowers makes final decisions based on its recommendations and conclusions.

The Policy as introduced will, therefore, be in full force and effect following contractual terms, including provisions that have been considered under Poland appendix.

1. Overview of Argentina Whistleblowing legislation:

In Argentina, no specific federal laws are solely dedicated to whistleblowing processes. However, several legal provisions indirectly support such implementations. These regulations have just been analyzed for the purpose of this policy to understand alignment, but due to contractual terms, collaborators from Argentina are conveyed under EU processes

1.1. The listed act can affect the interpretation of the Policy and its effects:

1.1.1. Repentant Law, Law No. 27,304 of 2016 ("**the Repenant Law**");

1.1.2. Complex Crimes Law, Law No. 27,319 of 2016 ("**the Complex Crimes Law**");
1.1.3. Witness Protection Law, Law No. 25,764 of 2003 ("**the Witness Protection Law**");
1.1.4. Criminal Code, Law No. 11,179 of 1984 ("**the Criminal Code**");
1.1.5. Personal Data Protection Act, Act No. 25,326 of 2000 ("**the PDP Act**");
1.1.6. Decree No. 1558/2001 Regulating the PDP Act;
1.1.7. Labour Contract Law, Act No. 20,744 of 1976 ("**the Labour Contract Law**");
1.1.8. Corporate Criminal Liability Law, Law No. 27,401 ("**the CCL Law**");
1.1.9. Money Laundering Law: 25,246 of 2000
1.1.10. Right to access public information: 27,275 of 2016;
1.1.11. Decree 206/2017 Regulating Right to access public information;
1.1.12. Decree 290/2007 Regulating Money Laundering Law;
1.1.13. Anti-Corruption Office Guidelines for the implementation of integrity programs;
1.1.14. Decree No. 62/2019 on Procedural Regime for Civil Forfeiture ("**the Civil Forfeiture Decree**");
1.1.15. Antitrust Law, Law No. 27,442 of 2018 ("**the Antitrust Law**"); and
1.1.16. regulations issued by the Argentinian Data Protection Authority ("**AAIP"**) may be applicable.

1.2. In addition to complementing the protective-oriented measures, positive incentives to whistleblowers have also been established by legislation. On the one hand, the Repentant Law foresees that persons investigated for corruption and other complex crimes (except high ranking State officials) may obtain a reduction of their punishment and the avoidance of a prison sentence during the process in exchange for the disclosure of precise, useful, and verifiable information relating to other participants in the offense and who occupied a higher hierarchical role in the criminal organization.

The Repentant Law has been effectively applied and has provided great visibility to the anti-corruption agenda. The Repentant Law makes the Witness Protection Program applicable to whistleblowers. In order to enjoy whistleblower protection under the Witness Protection Law, the individual must be either charged for the crimes provided by law or act as a witness. Under the Repentant Law, the individual must be an author or contributor to the crimes set forth in Article 1 of the Repentant Law.

Similarly, the Complex Crimes Law allows 'informants' to provide information and documentation related to organized crime to the police and other law enforcement agencies in exchange for a reward (Article 13 of the Complex Crimes Law). Under the Complex Crimes Law, as mentioned above, an informant shall be any person who provides relevant information to police authorities in order to initiate or guide the investigation regarding a crime listed in the Complex Crimes Law.

When it comes to corporate internal whistleblowers, the CCL Law encourages companies to establish a procedure for internal reporting so that employees and third parties can file reports anonymously and without fear of retaliation (Article 23(c)(III) and (IV) of the CCL Law). Concerning corporate whistleblowing, the Guidelines establish that reporting channels have to be properly accessible to all employees as well as to third parties and related parties (e.g.

vendors, suppliers, and business partners). However, the implementation of whistleblower protection programs is not mandatory for companies.

The CCL Law establishes that corporations may conduct internal investigations with due respect to the rights of the persons under investigation and imposes effective sanctions in case of violations of the internal policies or applicable laws (Article 23(c)(V) of the CCL Law). The Guidelines establish that internal corporate policies should clearly inform employees about company´s sanctioning regime and the general internal investigation procedure. Furthermore, the Guidelines establish that if a company decides to conduct an internal investigation, it is essential that the investigation process observes the limits arising from employees' rights, namely their privacy and dignity (Articles 70 and 72 of the Labour Contract Law) which the given Policy is compliant with. Information management must comply with the rules on gathering and handling personal information. There must be a balance between the right to investigate and the protection of privacy and dignity. In addition, the Guidelines establish that it is important that internal investigations respond to a written internal protocol previously approved by the board of directors, and previously communicated and agreed with the potential investigated persons in the form of a written agreement. Such an agreement must include allowing the company to access the sources and devices provided to the employees to perform their work. Employees must be warned about the fact that information stored in such sources or devices is the property of the Proprietary/Internal corporation, and that no privacy is to be expected in the event that these are used for personal or illicit purposes. The Guidelines also set up an investigation protocol, regulating areas such as the chain of custody of the gathered information, how electronic evidence should be handled, and witness interviews, among others. The procurement of outside counsel to conduct the investigation is advisable, especially when the allegations involve senior management, are particularly serious, or may have severe reputational consequences – as referred in the Policy, a member of the legal team is included in the Case Review Unit. In any case, it should be noted that internal investigations are a new feature in Argentine domestic law. The current state of case law is quite unbalanced in favour of employees due to Argentina's robust labour and data privacy protections.

Additionally, the Antitrust Law provides that any person who has committed or is in the process of committing any of the offenses listed in Section 2 of the Antitrust Law may disclose and acknowledge such conduct before the Competition Tribunal in exchange for an exemption or reduction of the sanctions set forth in the Antitrust Law. However, it is worth noting that the aforementioned Competition Tribunal has not been created yet, and the Secretary of Domestic Trade has not regulated the operative details of its leniency program. In order to enjoy the benefits set out in Article 60 of the Antitrust Law, the person reporting the conduct must have performed or be currently performing the action prescribed.

Therefore, there are no clear rules on how the whistleblowers' protection framework will be enforced yet. In addition, and according to the Property Decree, which sets a procedural regime for civil action, the Public Prosecutor's Office ('MPF') may develop collaboration programs with the persons who provide relevant information for asset recovery proceedings. The collaborating

persons may be awarded up to 10% of the goods obtained as a consequence of the information they provide.

2. **Procedure and timeliness of the handling of the submission**:

2.1. Deadline for acknowledgment of receipt of the submission - **immediately**, automatically or, in case of other available channels, on the day of receipt of the submission;
2.2. Deadline for acknowledgment of acceptance for processing (or rejection if there are insufficient grounds) / request for completion - **7 days** from receipt of application;
2.3. Deadline for feedback and follow-up - maximum **3 months** from the date of receipt of the submission. This time limit may be extended to **6 months**, if necessary, if the circumstances of the case and the nature of the problem reported require a longer procedure, in which case the reasons for the extension should be properly documented and communicated to those concerned.
2.4. The investigation should be finalized with a report, including recommendations for a decision on the pending submission. The report shall be forwarded within **7 days** of its completion to the parties concerned and to the relevant board Member designated for whistleblowers. The Relevant Board Member designated for whistleblowers shall, within 7 days after receipt of the report regarding its recommendations and bound by its conclusions, make the final decisions on the next steps and resolution of the case.

3. **What we provide under the Policy in the context of Argentina**:

3.1. As the freedom to regulate is vested in Spyrosoft – an internal whistleblower, who informs or reports to the higher authority (Whistleblowing Officer), where the wrongful act is being done, **will be guaranteed equal rights internally as regards confidentiality (including anonymity) and any rights to protection against retaliation which we are able to provide, analogous to those under the EU Directive**. In support of internal whistleblowers, Spyrosoft will provide appropriate information and legal resources to support the whistleblower in reporting and dealing with the adopted Policy. **You will not be left alone**.
3.2. In general, an Argentinian whistleblower's understanding is generally understood to be a person who has first-hand information about fraud or other kinds of misbehavior or unethical activity or wrongdoing within an organization and discloses the same in the overall interest of the organization and all its stakeholders. **There are no limitations or qualifications on who can be a whistleblower.** Any person with knowledge of a breach or wrongdoing may report it and qualify as a whistleblower, what is more – a whistleblower does not have to be a direct witness of the violation, the information may be independently assessed and acted upon, notwithstanding the fact that the whistleblower was not a first-hand witness to the reported act. We, therefore, accept any type of application that falls within the scope of our Policy.
3.3. In summary - our internal organs (Whistleblowing Officer, Champion, Case Unit Review team & dedicated Board Member), organized for the purpose of protecting and providing reporting options for whistleblowers, will provide you with the full range of intra-corporate assistance that you would be entitled to under European conditions. In case of any negative consequences - we have the tools and ability to enforce them internally at Spyrosoft and protect you from any retaliation. **Do not hesitate to speak up!**

3.4. As part of the national procedure in Argentina, Spyrosoft also covers violations arising from labour law in its broadest sense and the whistleblower protection associated with reporting them - under Procedure.

Personal data and processing information - Argentina legislation states it is unnecessary to notify the Data Protection Authority ("DPA") or seek approval from any agency to set up whistleblower programs. Nevertheless, if the whistleblower program includes creating a database with the employees' personal information, the company must comply with the requirements of the PDP Act. Having reviewed these, such requirements align with what is included in EU Data Privacy legislation.

Appendix 1.5 – Croatia

This Annex indicates the individual provisions, conditions and rules of the Policy specific to the country indicated in the title of the Annex. Please note that in the event of any dispute or inconsistency with national regulations, the provisions of the national regulations take precedence over the provisions of the Policy.

Timeline overview

Procedure and Timeliness	Deadline
Deadline for acknowledgment of receipt of the submission	**Immediately**, automatically, or on the day of receipt
Deadline for acknowledgment of acceptance for processing or rejection/request for completion	**7 days** from receipt of application
Deadline for feedback and follow-up	Maximum **30 days** from the date of submission, with a **possible extension to 90 days** if necessary. Reasons for extension must be documented and communicated.
Finalization of investigation and report	Report to be forwarded within **7 days** of completion of the investigation
Final decision on next steps and resolution	Within **7 days** of receiving the report, the Relevant Board Member designated for whistleblowers makes final decisions based on its recommendations and conclusions.
Informing the external reporting authority (Ombudsman)	Within **30 days** of the decision on the report, inform the external reporting authority (i.e., the Ombudsman) in writing about the report received and the outcome of the procedure.

1. **Relevant national provisions** – **The Act on Whistleblowers' Protection** (Official Gazette No. 46/2022) ('**the WP Act**') entered into force in Croatia on 23 April 2022, which implements Directive 2019/1937.

2. **Supervisory authority & external channel & support** – the whistleblowers may report the irregularity to the Ombudsman of the Republic of Croatia without previously using the mechanism of internal reporting. Reporting irregularities to the competent public authority (so-called "external reporting"), i.e. to the ombudsman is possible, either after the report has been submitted through the internal reporting system, or directly; whereas the internal whistleblowing procedure established by the organization (employer) is based on the reporting on irregularities submitted to the person of confidence appointed by the organization (employer). The Ombudsman is mandated to provide general legal information regarding the procedures and the channels for the reporting

of irregularities and public disclosure as well as protection measures available to the reporting persons under the Act

3. **Personal scope of whistleblower protection** – within the meaning of Croatian WP Act, the whistleblower could be bound with Spyrosoft via various contracts or relations including employment, self-employment, work outside employment (e.g. based on a service contract, engagement through an employment agency, etc.), volunteering, student work, participation in the recruitment process as a candidate, holders of stocks or shares in a company, persons who are members of the supervisory, management, or other bodies/boards of the company, persons who work under supervision and in accordance with the contractor's or vendor's instructions, as well as any other persons participating in activities of a natural or legal entity.

4. Person of confidence & employee's entitlements

4.1. If there is or will be constituted a work council in the company, **we ensure its right of co-determination.** If there is not – the **labour union representative**, or **at least 20% of employees** if no work council has been established or labour union representative has been appointed in Croatian companies of Spyrosoft. Before implementing the internal Policy, an appropriate consultation within the groups determined above will take place – which will determine the final version of the Croatian Policy.

4.2. The crucial position in the Policy lies in the role of the Whistleblowing Officer. According to Croatian law, reports on irregularities are submitted to the **person of confidence**, who also conducts the employer's internal whistleblowing procedure.

4.3. A person of confidence is an employee of the employer or a third natural person appointed by the employer for the purpose of receiving reports on irregularities, communicating with the whistleblower, and conducting the procedure regarding the reporting of irregularities.

4.4. A person of confidence and its deputy are appointed by the employer, on the initiative of either a work council or a labour union representative, or at least 20% of employees, if no work council has been established or labour union representative has been appointed at the workplace.

4.5. In case of a lack of such an initiative on the part of the work council/labour union representative or employees, the employer shall still appoint the person of confidence and their deputy (i.e. at its own discretion). However, such a position can be revoked, and the new person of confidence can be appointed at any time, on the subsequent initiative of the works council/labour union representative or at least 20% of employees.

4.6. Before their appointment, both the person of confidence and their deputy must give their prior written consent.

4.7. According to the WP Act, a person of confidence can also be a third natural person. Therefore, it would be possible to use the services of external service providers for the submission of a report and/or conducting an internal whistleblowing procedure, provided that the WP Act rules on the protection of identity, personal data, and confidentiality are always observed.

4.8. Transferring this to the Policy, **the following principles will be applied** to the staffing of Whistleblowing Officer and Whistleblowing Champion in this regard:

4.8.1. **Whistleblowing Officer would be suggested by the employer for approval** as the aim is to centralize this position for the group, naturally the proposal can be rejected and reelected;

4.8.2. **Whistleblowing Champion for Spyrosoft in Croatia would be elected by employees directly**. The Whistleblowing Officer is responsible for conducting the election and methods for its selection;

4.8.3. Both Officer and Champion will conclude adequate **confidentiality agreements** in this matter for the proper performance of its role.

5. **Procedure and timeliness of the handling of the submission**:

5.1. Deadline for acknowledgment of receipt of the submission - **immediately**, automatically or, in case of other available channels, on the day of receipt of the submission;

5.2. Deadline for acknowledgment of acceptance for processing (or rejection if there are insufficient grounds) / request for completion - **7 days** from receipt of application;

5.3. Deadline for feedback and follow-up - maximum **30 days** from the date of receipt of the submission. This time limit may be extended to **90 days**, if necessary if the circumstances of the case and the nature of the problem reported requiring a longer procedure, in which case the reasons for the extension should be properly documented and communicated to those concerned.

5.4. The investigation should be finalized with a report, including recommendations for a decision on the pending submission. The report shall be forwarded within **7 days** of its completion to the parties concerned and to the relevant board Member designated for whistleblowers. The Relevant Board Member designated for whistleblowers shall, within **7 days** after receipt of the report regarding its recommendations and bound by its conclusions, make the final decisions on the next steps and resolution of the case.

5.5. At the end step – inform the external reporting authority (i.e. the Ombudsman) in writing about the report received and the outcome of the procedure within **30 days** of the decision on the report.

5.6. Reports must be kept in a durable form in accordance with the national law governing the protection and processing of documentation and dossiers.

6. **Anonymous submissions - generally, the WP Act does not recognize anonymous whistleblowing, since one of the report's mandatory contents must be information about a person submitting the report.** However, as an exception, if an anonymous report has been submitted in a situation where (i) all other conditions laid down by the WP Act for qualifying for the protection of a whistleblower have been fulfilled, (ii) the identity of a whistleblower is subsequently determined, and (iii) they suffer retaliation, despite of anonymous reporting, the whistleblower in question shall also be entitled to the protection laid down by the WP Act.

7. **Additional whistleblowers entitlements**:

7.1. Right to request and receive **primary legal aid**;

7.2. Whistleblowers are entitled to protection before the court if there was a harmful action or retaliation undertaken towards them in relation to their report. In such a court procedure, a whistleblower can ask for:

7.2.1. The prohibition of further harmful actions/retaliation;

7.2.2. Compensation of damages; and

7.2.3. The publication of a court judgment in media.

Appendix 1.6 – Germany

This Annex indicates the individual provisions, conditions and rules of the Policy specific to the country indicated in the title of the Annex. Please note that in the event of any dispute or inconsistency with national regulations, the provisions of the national regulations take precedence over the provisions of the Policy.

Timeline overview

Procedure and Timeliness	Deadline
Deadline for acknowledgment of receipt of the submission	**Immediately**, automatically, or on the day of receipt
Deadline for acknowledgment of acceptance for processing or rejection/request for completion	**7 days** from receipt of application
Deadline for feedback and follow-up	Maximum **3 months** from the date of submission, with a **possible extension to 6 months** if necessary. Reasons for extension must be documented and communicated.
Finalization of investigation and report	Report to be forwarded within **7 days** of completion of the investigation
Final decision on next steps and resolution	Within **7 days** of receiving the report, the Relevant Board Member designated for whistleblowers makes final decisions based on its recommendations and conclusions.

1. **Procedure and timeliness of the handling of the submission**:

1.1. Deadline for acknowledgment of receipt of the submission - **immediately**, automatically or, in case of other available channels, on the day of receipt of the submission;

1.2. Deadline for acknowledgment of acceptance for processing (or rejection if there are insufficient grounds) / request for completion - **7 days** from receipt of application;

1.3. Deadline for feedback and follow-up - maximum **3 months** from the date of receipt of the submission. This time limit may be extended to **6 months**, if necessary, if the circumstances of the case and the nature of the problem reported require a longer procedure, in which case the reasons for the extension should be properly documented and communicated to those concerned.

1.4. The investigation should be finalized with a report, including recommendations for a decision on the pending submission. The report shall be forwarded within **7 days** of its completion to the parties concerned and to the relevant board Member designated for whistleblowers. The Relevant Board Member designated for whistleblowers shall, within 7 days after receipt of the report regarding its recommendations and bound by its conclusions, make the final decisions on the next steps and resolution of the case.

2. Internal Work Council – Germany
   2.1. If there is or will be constituted a work council in the company, we ensure its right of co-determination. A work council member selected independently will join the Case Unit Review team and proceed with the submission for the investigation and final report. Obviously, the said member would be bound with adequate measures of confidentiality obligations by a written agreement.

3. However, German law does not oblige companies to facilitate anonymous reporting. Spyrosoft declares that every submission will be processed in due course.

4. Scope of whistleblowers' reports covered - Sec. 2 HinSchG regulates which whistleblower reports are covered. In short, this includes all references to "significant violations". Criminal offenses and administrative offenses are included, as well as other regulations specified in Sec. 2 HinSchG - administrative offenses. However, the HinSchG only applies to administrative offenses because the violated regulation serves to protect the life, limb, health or the rights of employees or their representatives (e.g., works council members). Violations of (only) internal company policies and requirements are excluded from the scope of protection. It is important, however, that the reported or disclosed violation occurred in the context of a professional, entrepreneurial, or administrative activity (Sec. 3 para. 2 HinSchG). Accordingly, the HinSchG only applies to reports and disclosures that relate to the company or other entity with which the whistleblower was in contact as a result of his or her professional activities (Section 3 para. 3 - 5 HinSchG). However, we are extending the scope of permitted submissions to those set out in the Policy's assumptions, for the full protection and support of whistleblowers in the process of dealing with and reporting infringements. Additionally, as part of the national procedure in Germany, Spyrosoft also covers violations arising from labour law in its broadest sense and the whistleblower protection associated with reporting them - under Procedure.

5. Relationships between particular laws & preferred notification system
   5.1. Due to the fact that there are several specific laws protecting confidentiality, particularly regarding corporate trade secrets or contractual confidentiality obligations, we strongly encourage the use of the internal reporting structure introduced by the Policy, which provides a much higher level of protection for the whistleblower, in the case of matters bordering on different branches of law.
   5.2. In Germany, the aim of the protection for whistleblowers when facing retaliation is implementing a rule of reversal burden of proof. If a whistleblower suffers a disadvantage in connection with his or her professional activities and claims to have suffered such disadvantage as a result of a report or disclosure under this Act, such disadvantage shall be presumed to be a reprisal for such report or disclosure. This means that in such cases the employer must prove that its actions were in no way connected to the report or disclosure made (reversal of the burden of proof). However, the whistleblower must demonstrate and prove that a measure constitutes a disadvantage. What is more, there are a few exceptions, where protection could be limited.
   5.3. These exceptions result from:

5.3.1. **Security interests as well as confidentiality and secrecy obligations** - they take precedence over the HinSchG (e.g. Confidentiality obligations of lawyers, notaries or doctors and pharmacists);

5.3.2. **Trade secrets** - Persons who have acquired trade secrets or confidential information in a professional context, therefore, only enjoy protection under the HinSchG if they meet the requirements of this Act and the disclosure of the trade secret was necessary to uncover an infringement within the material scope of this Act. The disclosure of trade secrets or confidential information is therefore permitted.

5.3.3. **Last resort** - A whistleblower who discloses information to the public can only invoke whistleblower protection if the company (internal) and/or the authority (external) have not taken appropriate measures within the timeframe provided for or, in exceptional cases, if there is sufficient reason to believe that the public interest is at risk, there is a fear of reprisals or there is no prospect of clarification.

5.4. For the external reporting body – the German Government has established an office for external report at the **Federal Office of Justice (BfJ)**, where you can also submit notices. However, please acknowledge that the preferred channel of reporting is an internal one, as it is more effective and company-oriented.

6. Provisions on the processing of personal data:

6.1. Internal and external reporting channels are only authorized to process personal **data as far as necessary for the fulfillment of their tasks as specified in the German Whistleblower Protection Act. In addition, the processing of special categories of personal data is allowed—as an exception to Article 9 of the General Data Protection Regulation (GDPR)—if necessary for the fulfillment of a reporting channel's tasks**. However, specific protective measures must be taken in such cases.

6.2. Furthermore, the GDPR and the **German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)** must be complied with. In particular, the principle of data minimization under Article 5 of GDPR must be observed. This means that personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

7. Reprisal matters:

7.1. Whistleblower protection is the core element of the HinSchG. Thus, it sets out a prohibition against reprisals (Sec. 36 Abs. 1 HinSchG). Even attempted or threatened reprisals are prohibited. A reprisal is any kind of disadvantage that occurs as a result of a report. The term “reprisal” covers not only dismissal and disciplinary measures, but also mobbing, discrimination, exclusion, and unequal treatment. To protect whistleblowers, the law provides for a reversal of the burden of proof if they experience disadvantages following a report or disclosure in connection with their professional activities. In this case, **the existence of a reprisal is presumed**.

7.2. A false suspicion in the context of a report or disclosure can have far-reaching consequences for those affected. The effects may no longer be completely reversible. Therefore, the injured parties are entitled to compensation for the damage resulting from an intentional or grossly

negligent false report or disclosure. In this context, it should be mentioned that **the disclosure of knowingly incorrect information can also lead to a fine of up to 20,000 euros**.

Appendix 1.7 - India

This Annex indicates the individual provisions, conditions, and rules of the Policy that are specific to the country indicated in the title of the Annex. Please note that in the event of any dispute or inconsistency with national regulations, the provisions of the national regulations take precedence over the provisions of the Policy.

Timeline overview

Procedure and Timeliness	Deadline
Deadline for acknowledgment of receipt of the submission	**Immediately**, automatically, or on the day of receipt
Deadline for acknowledgment of acceptance for processing or rejection/request for completion	**7 days** from receipt of application
Deadline for feedback and follow-up	Maximum **3 months** from the date of submission, with a **possible extension to 6 months** if necessary. Reasons for extension must be documented and communicated.
Finalization of investigation and report	Report to be forwarded within **7 days** of completion of the investigation
Final decision on next steps and resolution	Within **7 days** of receiving the report, the Relevant Board Member designated for whistleblowers makes final decisions based on its recommendations and conclusions.

India is not a member state of the EU and are not linked to EU legislation in this area. For this reason, Directive 2019/1937 does not apply to Indian legislation and, in order to have any basis for application, we must look only to the applicable national legislation. For this reason, in the case of India, the Policy's legality will first be determined by locally adopted laws that regulate the content and values covered.

Therefore, the policy as introduced will be in full force and effect, except for elements that could be considered contrary to the regulations, in which case the provisions of Indian law apply.

1. The Indian Acts relevant to the enforcement of the policy:

1.1 The only legislation dealing with the protection of whistleblowers in India are:

1.1.1 **the Companies Act 2013** (Companies Act), which mandates the incorporation of a whistleblower policy, but primarily only by listed companies;

1.1.2 **the Whistle Blowers Protection Act 2014** (Whistle Blower Protection Act). This Act provides a legal mechanism for reporting illegal, unethical, and illegitimate practices by members of an organization. However, the scope of the Act is limited to public servants and public sector undertakings.

To date, there are no specific laws dealing with the protection of whistleblowers applicable to private, unlisted companies or unincorporated entities and their employees. As employers are free to formulate and adopt a whistleblower policy – Spyrosoft implements the Policy as given. However, it must be underlined that not all of the rights reserved to whistleblowers can be adapted and enforced – that is why enforceability relies on Spyrosoft and the Whistleblowing Officer.

2. Procedure and timeliness of the handling of the submission:

2.1 Deadline for acknowledgment of receipt of the submission - **immediately**, automatically or, in case of other available channels, on the day of receipt of the submission;

2.2 Deadline for acknowledgment of acceptance for processing (or rejection if there are insufficient grounds) / request for completion - **7 days** from receipt of application;

2.3 Deadline for feedback and follow-up - maximum **3 months** from the date of receipt of the submission. This time limit may be extended to **6 months**, if necessary if the circumstances of the case and the nature of the problem reported requiring a longer procedure, in which case the reasons for the extension should be properly documented and communicated to those concerned.

2.4 The investigation should be finalized with a report, including recommendations for a decision on the pending submission. The report shall be forwarded within **7 days** of its completion to the parties concerned and to the relevant board Member designated for whistleblowers. The Relevant Board Member designated for whistleblowers shall, within 7 days after receipt of the report regarding its recommendations and bound by its conclusions, make the final decisions on the next steps and resolution of the case.

3. What we provide under the Policy in the context of India:

3.1 As the freedom to regulate is vested in Spyrosoft – an internal whistleblower, who informs or reports to the higher authority (Whistleblowing Officer), where the wrongful act is being done, **will be guaranteed equal rights internally as regards confidentiality (including anonymity) and any rights to protection against retaliation which we are able to provide, analogous to those under the EU Directive**. Of course, in cases where this is possible, the whistleblower will also be protected under local law. In support of internal whistleblowers, Spyrosoft will provide appropriate information and legal resources to support the whistleblower in reporting and dealing with the adopted Policy. **You will not be left alone**.

3.2 A general Indian whistleblower's understanding is generally understood to be a person who has first-hand information of fraud or other kinds of misbehavior or unethical activity or wrongdoing within an organization and discloses the same in the overall interest of the organization and all its stakeholders. **There are no limitations or qualifications on who can be a whistleblower.** Any person with knowledge of a breach or wrongdoing may report it and qualify as a whistleblower, what is more – a whistleblower does not have to be a direct witness of the violation, and the information may be independently assessed and acted upon, notwithstanding the fact that the whistleblower was not a first-hand witness to the reported act. We, therefore, accept any type of application that falls within the scope of our Policy.

3.3 As part of the national procedure in India, Spyrosoft also covers violations arising from labour law in its broadest sense and the whistleblower protection associated with reporting them - under Procedure.

3.4 We encourage you to speak up in any case you asses as infringing; however, be aware that mala fide intention within the company also could result in disciplinary sanctions. As to the external ones - persons who make any disclosure with a mala fide intention or knowing that it was incorrect or false or misleading, shall be punishable with imprisonment for up to two years and a fine of up to 30,000 rupees.

In summary - our internal organs (Whistleblowing Officer, Champion, Case Unit Review team & dedicated Board Member), organized for the purpose of protecting and providing reporting options for whistleblowers, will provide you with the full range of intra-corporate assistance that you would be entitled to under European conditions. In case of any negative consequences - we have the tools and ability to enforce them internally at Spyrosoft and protect you from any retaliation. **Do not hesitate to speak up!**

Appendix 1.8 – USA

This Annex indicates the individual provisions, conditions, and rules of the Policy specific to the country indicated in the title of the Annex. Please note that in the event of any dispute or inconsistency with national regulations, the provisions of the national regulations take precedence over the provisions of the Policy.

Timeline overview

Procedure and Timeliness	Deadline
Deadline for acknowledgment of receipt of the submission	**Immediately**, automatically, or on the day of receipt
Deadline for acknowledgment of acceptance for processing or rejection/request for completion	**7 days** from receipt of application
Deadline for feedback and follow-up	Maximum **3 months** from the date of submission, with a **possible extension to 6 months** if necessary. Reasons for extension must be documented and communicated.
Finalization of investigation and report	Report to be forwarded within **7 days** of completion of the investigation
Final decision on next steps and resolution	Within **7 days** of receiving the report, the Relevant Board Member designated for whistleblowers makes final decisions based on its recommendations and conclusions.

The USA is not a member state of the EU and is not linked to EU legislation in this area. For this reason, Directive 2019/1937 does not apply to US legislation, and in order to have any basis for application, we must look only to the applicable national legislation. For this reason, in the case of the US, the Policy's legality will first be determined by locally adopted laws that regulate the content and values covered.

The Policy as introduced will, therefore, be in full force and effect, except for elements that could be considered contrary to the regulations - in which case the relevant provisions of US law apply.

The United States has a very elaborate system of whistleblower protection legislation, divided by industry and case - different provisions apply depending on the basis of the notification. For this reason, the US annex focuses on the terms and conditions of the Policy, only further indicating general sources of information as to the application of the law in particular cases. In the EU, whistleblowing protection is relatively universal thanks to the EU Whistleblowing Directive (2019/1937), whilst whistleblowing protection in US is patchier and is dependent on the sector in which you work and what it is you wish to report.

1. **Adopted procedure and timeliness of the handling of the submission (Policy)**:

1.1. Deadline for acknowledgment of receipt of the submission - **immediately**, automatically or, in case of other available channels, on the day of receipt of the submission;
1.2. Deadline for acknowledgment of acceptance for processing (or rejection if there are insufficient grounds) / request for completion - **7 days** from receipt of application;
1.3. Deadline for feedback and follow-up - maximum **3 months** from the date of receipt of the submission. This time limit may be extended to **6 months**, if necessary, if the circumstances of the case and the nature of the problem reported require a longer procedure, in which case the reasons for the extension should be properly documented and communicated to those concerned.
1.4. The investigation should be finalized with a report, including recommendations for a decision on the pending submission. The report shall be forwarded within **7 days** of its completion to the parties concerned and to the relevant board Member designated for whistleblowers. The Relevant Board Member designated for whistleblowers shall, within 7 days after receipt of the report regarding its recommendations and bound by its conclusions, make the final decisions on the next steps and resolution of the case.

2. Main principles of internal whistleblowing channels in US:

2.1. There is no general legal requirement to create whistleblower policies, but companies that are potentially subject to SOX, DFA, AMLA or other federal or state whistleblower requirements should ensure that they are prepared by creating policies and procedures that address how they will respond to and protect whistleblowers. These policies and procedures must be appropriately tailored to take into account factors such as the size of the company, the statutory whistleblower provisions that apply and the nature of its business – and so Spyrosoft Policy is.
2.2. Once a company learns that a whistleblower report has been made, it should adhere to its whistleblower policy. First, the company should assess the whistleblower's claim to determine what responsive action is appropriate. As discussed above, the nature of the inquiry will depend on the claim but could range from an informal assessment by the compliance team to a formal investigation conducted by external counsel. Ultimately, the determination of how to investigate the claim will depend on the severity of the alleged conduct and the credibility of the claim. In conducting the inquiry, it is critical that the company makes clear to any employees who are interviewed that even though the substance of the interview may be protected by the company's attorney-client privilege, the employee retains the right to disclose the facts discussed during the interview to the appropriate authorities. Second, in the case of a whistleblower report by an employee whose identity is known, in addition to the steps outlined in the whistleblower policy to protect the employee, the company should also ensure that it has documented any previous warnings or disciplinary actions taken against the employee, and adhere to consistent disciplinary procedures. Such documentation and adherence will, if necessary, support the company's position that a whistleblower employee was disciplined or dismissed for conduct unrelated to a whistleblower report.
2.3. It is also worth to underline that – depending on the case, circumstances, and matter, the US system rewards whistleblowers (monetary reward) for detecting and correctly reporting irregularities. This should be kept in mind and verified against the case under review.

2.4. Best practices – 4 steps for whistleblowing law in the US, which the company could introduce independently are:

2.4.1. Confidentiality—A common thread throughout whistleblowing protection legislation, anonymity/confidentiality has the twin benefits of protecting whistleblowers from retaliation and encouraging them to speak up in the first place.

2.4.2. Offering a reward - In many cases, whistleblowers provide information that allows prosecutors to recuperate money. It is advised that whistleblowers are offering a portion of this money as a reward for their courage and to encourage others to follow suit.

2.4.3. Remediation in cases of retaliation - These are measures to mitigate the damages a whistleblower may face after speaking out. They include back pay, being reinstated in their job if unfairly fired, front pay (when finding a new job), out-of-pocket losses, and so on.

2.4.4. Independent reporting channels - Allows whistleblowers to submit reports to a neutral third-party.

In Spyrosoft pt 1, 3-4 are guaranteed and pt 2 could be implemented if necessary.

3. Important legislation & where to find help/support while determining a submission:

3.1. When it comes to legislation, there are several US Acts, which are crucial to the whistleblower's protection (could also relate and apply to the said Policy):

3.1.1. **The Whistleblower Protection Act** (1989) is the broadest piece of legislation introduced in the US, but it does not provide protection for all whistleblowers, far from it. The Whistleblower Protection Act **only protects federal employees, although private sector workers may be protected under topic-specific federal laws**, like the Occupational Safety and Health Act, but only a small section of unlawful activity is covered by such laws. **Private sector workers do not enjoy any kind of whistleblowing protection if they are reporting violations of federal laws with no whistleblower protection or state law**. However, there may be some protection for them under local laws. **Moreover, in the US, union officials are exempted from whistleblower laws**.

3.1.2. **The False Claims Act (FCA)** - '**Qui tam**' is the whistleblower provision of the FCA. It originates from Latin and is an abbreviation for a longer phrase meaning "Who sues on behalf of the King as well as for himself." Put simply, qui tam means that a private citizen initiates legal action on behalf of the state. Qui tam enables employees to blow the whistle on those committing fraudulent activity against the government and file a lawsuit on behalf of the government. If the case is successful, the government will recover their lost funds in damages and penalties. Qui tam entitles whistleblowers to receive a share of the recovered funds, protection against employer retaliation as well as recovered legal fees and costs. It is important to note that if the US government decides not to investigate claims, the whistleblower can undertake private action and file a lawsuit independently.

3.1.3. **The Dodd-Frank Act -** The Dodd-Frank Act is not a whistleblowing act; however, there are whistleblowing components as employees are extremely helpful and well-placed in bringing fraudulent activity to the attention of authorities. The Dodd-Frank Act strengthened the whistleblower programme that had been introduced by SOX, to provide greater provisions and protections for whistleblowers. Changes include: a) broadening the types of employees covered by the whistleblower program to include the employees of a

company's subsidiaries and affiliates; b) increasing the statute of limitations to 180 days after the violation was discovered for an employee to bring forward a whistleblowing claim against their employer; c) forming a rewards programme through which whistleblowers are entitled to 10-30% of the recovered funds from a successful case.
Whistleblowers are encouraged to disclose "original" information about fraudulent activities committed by their employer, in the name of economic fairness. The information must be acquired independently by the whistleblower, not from previous allegations in the media, news, reports or hearings for example. The Dodd-Frank Act created two commissions through which whistleblowers can report violations - The US Securities and Exchange Commission (SEC) and The Commodity Futures Trading Commission (CFTC).
However, unlike the False Claims Act, whistleblowers are not allowed to make independent investigations under the Dodd-Frank Act. Once claims of wrongdoing have been filed by a whistleblower, it is the responsibility of the SEC or CFTC to investigate the allegations. The whistleblower cannot take private action if the SEC/CFTC decides not to investigate or press sanctions.

Also, as part of the national procedure in USA, Spyrosoft also covers violations arising from labour law in its broadest sense and the whistleblower protection associated with reporting them - under Procedure.

However, it should be borne in mind that these are only the most important foundations of the system, which consists of many more minor laws. In the event of disputes/doubts about the correctness of the Policy's actions - Spyrosoft will analyse case by case individual cases and proceedings.

3.2. Useful links and support:

3.2.1. https://www.dol.gov/general/topics/whistleblower - US Department of Labor offers wide protection information, especially with regard to the anti-retaliation proceedings. There are over 16 different branches, where you can find necessary information for further proceedings. What is more, U.S. Department of Labor is an organization of diverse functions that carries out its mission through a number of offices and agencies. Five agencies enforce whistleblower and anti-retaliation laws:

3.2.1.1. Occupational Safety and Health Administration (OSHA);
3.2.1.2. Mine Safety and Health Administration (MSHA);
3.2.1.3. Office of Federal Contract Compliance Programs (OFCCP);
3.2.1.4. Wage and Hour Division (WHD);
3.2.1.5. Veterans' Employment and Training Service (VETS).

Each covering several displayed issues.

3.2.2. https://oig.justice.gov/hotline/whistleblower-protection - US Department of Justice Office (DOJ) of the Inspector General, which supports submissions through DOJ.

3.2.3. https://osc.gov/ - consultancy with US Office of Special Counsel on the whistleblowing issues with prepared and fundamental matters related to disclosure of wrongdoing.

Appendix 1.9 – Norway

This Annex indicates the individual provisions, conditions, and rules of the Policy that are specific to the country indicated in the title of the Annex. Please note that in the event of any dispute or inconsistency with national regulations, the provisions of the national regulations take precedence over the provisions of the Policy.

Timeline overview

Procedure and Timeliness	Deadline
Deadline for acknowledgment of receipt of the submission	**Immediately**, automatically, or on the day of receipt
Deadline for acknowledgment of acceptance for processing or rejection/request for completion	**7 days** from receipt of application
Deadline for feedback and follow-up	Maximum **3 months** from the date of submission, with a **possible extension to 6 months** if necessary. Reasons for extension must be documented and communicated.
Finalization of investigation and report	Report to be forwarded within **7 days** of completion of the investigation
Final decision on next steps and resolution	Within **7 days** of receiving the report, the Relevant Board Member designated for whistleblowers makes final decisions based on its recommendations and conclusions.

Norway is not a member state of the EU but is associated with the Union by membership in the European Economic Area (EEA). When the EU adopts directives regulating the internal market, these must also be included in the EEA agreement and, as a result, implemented in Norwegian legislation. The Whistleblowing Directive is still under scrutiny by EEA/EFTA, who are considering its relevance for the EEA and whether it will be included in the EEA agreement.
For this reason, in Norway, the Policy's legality will first be determined by locally adopted laws that regulate its content and values.
Norwegian employment legislation already protects employees who report on their working conditions. However, Norway does not have a designated Whistleblowing Act that offers protection to a wider range of persons than employees or hired employees.
The Policy as introduced will, therefore, be in full force and effect, except for elements that could be considered contrary to the regulations - in which case the provisions of Norwegian law apply.

1. The Norwegian Acts relevant to the enforcement of the policy:

   1.1. **The Norwegian Working Environment Act (WEA—Chapter 2A) mainly covers a scheme for employees to report** on censurable conditions as defined in the WEA.

1.1.1. Under these provisions, employees are entitled to report censurable conditions in the undertaking. In addition to employees, a number of other personnel groups are regarded as employees in terms of whistleblowing, such as students, military personnel, inmates, patients, and persons who, for training purposes or in connection with work-oriented measures, are placed in undertakings without being employees and persons participating in labour market schemes. Censurable conditions include, among others, breaches of law or other ethical standards, such as danger to life and health, climate or environmental hazard, corruption or other financial crime, dangerous working environment, harassment and breach of personal data security. Whistleblowing exclusively related to an employee's own employment is not covered by the definition of censurable conditions.

1.1.2. Under Norwegian law employees are also required to report harassment and discrimination as well as risks to life or health. Any form of retaliation against a whistleblower is prohibited, and any breach in this regard is subject to liability for economic and non-economic damages. The employer has to investigate whistleblower complaints within a reasonable time and employers with five or more employees are obligated to establish a written whistleblowing procedure.

1.1.3. The main difference between the Whistleblowing Directive and the current Norwegian legislation is that the Whistleblowing Directive covers a wider sphere of personnel, but includes a more limited selection of topics the whistleblower complaints may address. New rules are also introduced, for instance, concerning whistleblowing channels.

1.2. Norwegian Personal Data Act (*Personopplysningsloven*) – with regard to the coverage of processing of personal data when handling whistleblowing reports.

1.2.1. The relevant legal bases for processing personal data in relation to whistleblowing under the GDPR are Art. 6.1 c) compliance with a legal obligation and f) legitimate interest. Special categories of personal data can be processed if this is necessary to comply with the employer's obligations and rights pursuant to the Norwegian Personal Data Act, Section 6.

2. Procedure and timeliness of the handling of the submission:

2.1. Deadline for acknowledgment of receipt of the submission - **immediately**, automatically or, in case of other available channels, on the day of receipt of the submission;

2.2. Deadline for acknowledgment of acceptance for processing (or rejection if there are insufficient grounds) / request for completion - **7 days** from receipt of application;

2.3. Deadline for feedback and follow-up - maximum **3 months** from the date of receipt of the submission. This time limit may be extended to **6 months**, if necessary, if the circumstances of the case and the nature of the problem reported require a longer procedure, in which case the reasons for the extension should be properly documented and communicated to those concerned.

2.4. The investigation should be finalized with a report, including recommendations for a decision on the pending submission. The report shall be forwarded within **7 days** of its completion to the parties concerned and to the relevant board Member designated for whistleblowers. The Relevant Board Member designated for whistleblowers shall, within 7 days after receipt of the report regarding its recommendations and bound by its conclusions, make the final decisions on the next steps and resolution of the case.

3. Tips for reporting violations in Norway:
   3.1. As vesting in the WEA, everyone working in Norway has the right to notify censurable conditions. However, it is also a duty, meaning that you actually have no choice if the matter is serious enough (which includes temporary employees hired from agencies).
   3.2. Collect evidence—When considering reporting censurable conditions, it is smart to collect as much evidence as possible. Saving e-mails, letters, and other documentation is very useful, therefore. Even recording a conversation can stand as evidence in further proceedings.
   3.3. The content determines if something can be classified as whistleblowing. Neither the format nor the wording should matter. However, it is crucial to make clear what is being notified during the procedure—don't leave room for doubt. We also recommend including the words "vessel," "whistleblowing," or "notification of censurable condition" while making a report.
   3.4. Be precise and credible – try to describe the matter as precisely as you can, and underline why you think it is serious. Enclose documentation and let us know if other people can confirm your claims.
   3.5. You can remain anonymous if you want to. However, it will make it harder to proceed with your report.

4. Supporting institution

   4.1. The Norwegian Anti-Discrimination Tribunal is a neutral party and a free alternative to judicial proceedings in cases of discrimination, harassment, and retaliation.
   4.2. The Norwegian Labour Inspection Authority is an informative authority, but you can also notify them directly about the subject matter.

Appendix 2
Data protection, data storage and information security

Given the fact that Spyrosoft hereby implements the Policy throughout the group, using an integrated tool designed to serve all of its entities under the rules set out therein, while maintaining the general terms and conditions and the distinctiveness of the proceedings in the individual entities - thus using the SpeakUp box, the Controller and the entity linking the entire system will be Spyrosoft S.A. in compliance with all obligations and regulations concerning the protection and processing of personal data.

I. General Information

1. The Controller of the data provided, disclosed, processed and protected in the adopted whistleblower system within the Policy is the relevant company within the Spyrosoft group to which the notification under this procedure is addressed, hereinafter referred to as the "**Controller**". These are:
    a. **Spyrosoft Spółka Akcyjna** with its registered office in Wrocław (50-141), Plac Nowy Targ 28, entered in the Register of Entrepreneurs kept by the District Court for Wrocław – Fabryczna in Wrocław, 6th Commercial Division, under KRS number: 0000616387, Tax Identification Number (NIP): 8943078149;
    b. **Spyrosoft Solutions Spółka Akcyjna** with its registered office in Wrocław (50-141), Plac Nowy Targ 28, entered in the Register of Entrepreneurs kept by the District Court for Wrocław – Fabryczna in Wrocław, 6th Commercial Division, under KRS number: 0000724282, Tax Identification Number (NIP): 8992842857;
    c. **Spyrosoft Solutions GmbH** with its registered office in Stuttgart (70563), Curiestrasse 2, Germany, registered under number: D-U-N-S 343156804, Tax Identification Number (NIP): 143/182/41911;
    d. **Spyrosoft Solutions d.o.o.** with its registered office in Grada Vukovara 284, Ulaz B, 4. Kat, 10000 Zagreb, Croatia, registered by Croatian Commerce Court under Business subject number: 081239880, Tax Identification Number (NIP): HR39610495870;
    e. **Spyrosoft Solutions S.R.L.** with its registered office in Bd. Liviu Rebreanu 76-78, 300755 Timisoara, Romania, registered under number: J35/1161/2022, Fiscal Code: 45812482;
    f. **Spyrosoft Solutions LLC** with its registered office in 301 East Liberty Street, Suite 500, Ann Arbor, NI, 48104, USA, registered under Company number: 802276489;
    g. **Spyrosoft LTD** with its registered office in Smartbase, Target Way, Aviation Park West, Christchurch, BH23 6NW, United Kingdom VAT number: GB232467221;
    h. **Spyrosoft Synergy Spółka Akcyjna** with its registered office in Szczecin (71-441), ul. Cyfrowa 4, entered in the Register of Entrepreneurs kept by the District Court for Szczecin-Centre in Szczecin, 6th Commercial Division of the National Court Register, under KRS number: 0000946182, Tax Identification Number (NIP): 8513265624;
    i. **Spyrosoft Ecommerce Spółka Akcyjna** with its registered office in Wrocław (50-141), Plac Nowy Targ 28, entered in the Register of Entrepreneurs kept by the District Court for Wrocław – Fabryczna in Wrocław, 6th Commercial Division, under KRS number: 0000982635, Tax Identification Number (NIP): 8971905305;
    j. **Spyrosoft Connect Spółka Akcyjna** with its registered office in Wrocław (50-141), Plac Nowy Targ 28, entered in the Register of Entrepreneurs kept by the District Court for Wrocław – Fabryczna in Wrocław, 6th Commercial Division, under KRS number: 0001021782, Tax Identification Number (NIP): 8971917490;

k. **Spyrosoft India Private Limited** with its registered office in Tamil Nadu, 1320, flat no 3b main road anna nagar west chennai, Egmore Nungambakkam, India (600040), registration number: 154301, CIN: U72900TN2022FTC154301;
l. **Spyrosoft BSG Spółka Akcyjna** with its registered office in Wrocław (50-141), Plac Nowy Targ 28, entered in the Register of Entrepreneurs kept by the District Court for Wrocław – Fabryczna in Wrocław, 6th Commercial Division, under KRS number: 0000602767, Tax Identification Number (NIP): 8971820046;
m. **Spyrosoft BSS Spółka z ograniczoną odpowiedzialnością** with its registered office in Wrocław (50-141), Plac Nowy Targ 28, entered in the Register of Entrepreneurs kept by the District Court for Wrocław – Fabryczna in Wrocław, 6th Commercial Division, under KRS number: 0000323476, Tax Identification Number (NIP): 5272593301;
n. **Unravel Spółka Akcyjna** with its registered office in Wrocław (50-141), Plac Nowy Targ 28, entered in the Register of Entrepreneurs kept by the District Court for Wrocław – Fabryczna in Wrocław, 6th Commercial Division, under KRS number: 0000842732, Tax Identification Number (NIP): 8971879134;
o. **GOD Nearshore SE Europejska Spółka Akcyjna oddział w Polsce** with its registered office in Wrocław (50-141), Plac Nowy Targ 28, entered in the Register of Entrepreneurs kept by the District Court for Wrocław – Fabryczna in Wrocław, 6th Commercial Division, under KRS number: 0000698141, Tax Identification Number (NIP): 0000698141;
p. **Finin Spółka z ograniczoną odpowiedzialnością** with its registered office in Wrocław (50-141), Plac Nowy Targ 28, entered in the Register of Entrepreneurs kept by the District Court for Wrocław – Fabryczna in Wrocław, 6th Commercial Division, under KRS number: 0000862063, Tax Identification Number (NIP): 8971883791.

2. The Controller hereby determines the purposes, methods, and safeguards for processing and conducting the processing of the personal and other data related to being reported in the whistleblower system.
3. You can contact the Controller in writing via traditional mail at the relevant address indicated under point 1(a-), or by email to the following address: SpeakUp@spyro-soft.com.
4. Your personal data is safe with us. Be sure that we process your data only via clearly defined channels indicated in the Policy – that is where the information is protected. Whistleblowers identity, who report serious wrongdoing or irregularities in good faith are treated with the utmost confidentiality and are protected against any retaliation. What is more, it will never be revealed except in certain exceptional circumstances if the whistleblower authorizes such a disclosure, if this is required by any subsequent criminal law proceedings, or if the whistleblower maliciously makes a false statement.

II. Objectives of whistleblower protection vs. GDPR policies

1. The Controller is mindful that any processing of personal data carried out in processes related to the whistleblower policy under Directive 2019/1937 must be done according to the GDPR. In view of this, in implementing the whistleblowing process and the protection of whistleblowers-within the Spyrosoft Group, the Controller has the following objectives to ensure that the data protection requirements set out in Article 5 of the GDPR are met:
    a. Ensure that the Policy is lawful about the processing and protection of personal data, is fair and transparent;
    b. Applying the principle of data minimization and using appropriate retention periods by archiving or deleting personal data that are clearly not relevant to the proceedings in a

particular case or are no longer required; archiving/deleting such data shall take place as soon as the indicated circumstances arise;

c. Maintaining a record of each request received - enabling this data to be securely managed, and traceable in the process, maintaining appropriate documentation of individual requests, and deleting/archiving this data;
d. Provide transparent and clear information to data subjects whose data will be processed as part of the notification (in accordance with Articles 13 and 14 of the GDPR);
e. Ensuring that data subjects' rights can be exercised, including - specifying the possibility of deferring or limiting them (for legitimate reasons);
f. Applying organizational and technical security measures appropriate to the risks and requirements of the law to ensure the confidentiality, integrity, and availability of the data, in particular, the confidentiality or anonymity of whistleblowers and all other persons involved;
g. Determination of appropriate retention periods depending on the type of notification identified;
h. Assess the appropriate competence of internal and external recipients and appropriately limit the transfer of personal data to necessary persons in accordance with the law or applicable rules;
i. Describing the process in the **Register of Processing Activities** (**RPA**);
j. Conduct a **Data Protection Impact Assessment** (**DIA**) for proceedings under the Policy.

This document identifies and ensures that the data protection objectives are met in the proceedings and data processing under the Policy.

III. Personal scope of data protection

The breach notification process involves the processing of the personal data of various individuals. This data may be recorded in the notification and may additionally be collected, analyzed, completed, reported, distributed, or deleted.

In accordance with the Policy's provisions, whistleblowers are ensured the right to privacy, particularly to protect them from repressive actions, discrimination, or other types of unfair treatment.

Upon receipt of a report of a breach, the Controller may collect and process the personal data of persons directly or indirectly affected by the report, even (in some cases) without their consent (the application of Article 14(2)(f) GDPR, is excluded in this regard). The scope of subjects in this case concerns the following persons:

a) Whistleblower,
b) Alleged perpetrator,
c) Witnesses,
d) Third parties (staff members or other persons who are merely quoted).

IV. Data Protection Impact Assessment (DIA)

The Controller, in order to maintain compliance with the processing requirements in terms of the Controller's legitimate interest (Article 6(1)(f) of the GPRD and recital 47 of the GDPR), shall, in each case, carry out an appropriate DIA analysis to verify whether the processing of your personal data on this basis is legitimate.

The results of conducting such a test, in each case, will be documented and stored at the RPA.

V. Grounds for data processing under the Policy

Your personal data collected under the Policy in the whistleblowing process is processed in accordance with the following grounds:

a) **necessity for compliance with a legal obligation** (Article 6(1)(c) GDPR) - as regards the fulfillment of legal obligations obliging the data Controller to establish and implement internal control procedures in the area of whistleblowers;
b) **the legitimate interest of the Controller or the third party to whom the data are disclosed** (Article 6(1)(f) GDPR) - to the extent necessary for its implementation in the case of an interest in the proceedings that goes beyond the legal obligation, in the event of a positive outcome of the assessment (OPUI assessment of the legitimate interest in accordance with Article 6(1)(f) GDPR and recital 47 GDPR) of such interest;
c) **consent** - in the event that the whistleblower discloses his or her identity (Article 6(1)(a) GDPR).

At the same time, following the principles of the Policy, we emphasize that a whistleblower:

- has the right to remain anonymous;

- may withdraw consent to the processing of his/her personal data at any time;

- withdrawal of consent does not affect the processing of data which took place prior to its withdrawal (in particular - after proceedings have been initiated);

- the whistleblower's personal data and that of any persons involved in ongoing proceedings are protected against unauthorized access.

VI. Information obligations

In fulfillment of the Controller's duty of information, Spyrosoft - as part of the fulfillment of its obligations regarding the Policy, in the context of investigations and when reporting them, will inform all persons related to the reported irregularity about the processing as soon as possible and in a transparent manner, i.e.: whistleblowers, the alleged perpetrator, witnesses and any third parties (where appropriate - members of staff or other persons who are merely quoted).

For this purpose, the Controller will prepare appropriate so-called information clauses to be attached to the content of the notification forms - in the case of notifications via traditional and electronic communication channels in writing, and in the case of notifications without forms in other forms - directly in response to the notification via the same communication channel (individual notification of the implementation of the process with the obligation to acknowledge reading of the message).

In addition, the information clauses can be found at Whistleblowing (sharepoint.com).

VII. Your rights in data processing under the Policy

All individuals whose data is processed in the whistleblower process are provided with a number of rights (arising, inter alia, from Articles 13 and 14 of the GDPR) that they can exercise in the process - these may be subject to certain limitations, due to the possible adverse effects on other individuals associated with the Policy process.

Controller, within the framework of ongoing proceedings, due to individual interest in certain cases (e.g. informing at a certain stage of the proceedings may be detrimental to the case, high risk of infringement, disclosure would hinder the procedure of dealing with the notification, etc.), may decide to defer or limit some of these rights. Any restriction/deferral applied will be duly documented in each individual case and justified for supervisory purposes.

You have the right to:

a) Access to data - Controller shall provide persons in the process with access to data as part of the implementation of the Policy, as long as this may not adversely affect the ability to conduct an investigation or expose other persons to negative consequences (retaliation, stigmatization, victimization). The extent of access will be appropriately tailored to the level of sensitivity of the data and the associated risks and the subject of the request;
b) Correction of data - if the request is justified, Controller will update or complete the data held if it is incomplete or out of date, taking also into account the perspective of the events of the persons involved, applying the principle of additional supplementary entries;
c) Objection - in the case of processing on the basis of a legitimate interest or in the public interest (Article 6(1)(e) and (f) GDPR), you have the right to object to such processing. The Controller will no longer be able to process them for this purpose unless he/she demonstrates the existence of a valid legitimate interest to process, overriding your interests, and documents it;
d) Deletion of data - similarly to point c), additionally, it may be restricted if the prerequisites of Article 17(3) GDPR apply (e.g. to protect the rights and freedoms of other persons affected by the notification, to comply with a legal obligation or in connection with a task carried out in the public interest);
e) Restrictions on data processing (pursuant to Article 18(1) of the GDPR).

VIII. Security rules for data protection

Your data is safe with us- the whistleblower system has been organized and implemented at Spyrosoft in such a way that through the use of appropriate technical and organizational safeguards- we can properly fulfill the responsibilities entrusted to us. The purpose of their implementation is, among other things, to protect data against accidental or unlawful destruction, loss, modification, unauthorized disclosure, or access to data transmitted, stored, or otherwise processed in order to ensure the highest possible level of data confidentiality and security. The Whistleblowing Officer, Whistleblowing Champions, and all members of the Case Unit Review have been appropriately trained and are responsible for the proper conduct of each of the proceedings on this subject.

Your personal data may be transferred to an entity providing hosting services to the Controllers, which has appropriate safeguards against third-party access to the data stored.

Your personal data will not be transferred to recipients located in a third country, i.e., outside the European Economic Area.
In terms of technical safeguards, by meeting the standards of the ISO 27000 family, we can ensure a professional and secure level of operations when implementing the policy's provisions.

In addition, to guarantee the security of your data and the correctness of the process, we operate according to the following rules:

a) **Lawfulness, reliability, and transparency** - ensuring that the processing of personal data is lawful, fair, and transparent for the data subject;
b) **Purpose limitation** - personal data collected in the context of a whistleblower notification may only be processed for specific and legitimate purposes;
c) **Data minimization** - we will ensure that we do not collect personal data that is not relevant to the handling of a particular application. Redundant data will be identified and deleted without undue delay;
d) **Security of data processing** —The introduction of secure channels for reporting irregularities ensures the security of data processing when reported. Information sharing will always take place through the designated channels delineated in the Policy. Those who have access to them have received dedicated training in this area and have been required in writing to maintain the confidentiality of the data and apply safeguards. Report data are only disclosed to those who need to access them for report investigation/ follow-up.
e) **Accuracy** - the Controller shall take steps to ensure that personal data is correct and, where necessary, kept up to date, as well as all reasonable steps to ensure that personal data that is incorrect in light of the purposes of its processing is promptly deleted or rectified;
f) **Data retention period — data will only be stored for the periods indicated for the data regions. After the expiry of these periods, the data will be deleted. They are processed until the purpose of their processing/consent** to their processing is withdrawn.
g) **Protection of relevant persons** - we ensure confidentiality, record individual reports and whistleblower reports, protect whistleblowers from retaliation, and offer support to whistleblowers- by providing support, information, and advice in proceedings before the competent authorities, including legal support.

The objectives referred to above shall be pursued by taking appropriate steps and applying effective safeguards, which shall include in particular:

- continuously raising the awareness and knowledge of individualls in the field of personal data security;
- communicating to individualls the consequences, including disciplinary, in the event of a personal data breach;
- assigning access to documents, materials or systems containing personal data only to authorized persons;
- securing documents, materials or systems against the loss or destruction of personal data contained therein;
- implementing detailed rules defining the method of user rights management and authentication rules in all systems operated by the Controller;
- reporting of information security incidents;
- regular risk analysis in the area of information security and designing activities to minimize potential risks;

Taking into account the state of technical knowledge, the cost of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of violation of the rights and freedoms of natural persons with different probabilities of occurrence and the severity of the threat resulting from processing, the Controller has implemented – both when determining the methods of processing and during the processing itself – appropriate technical and organizational measures, designed to effectively implement the principles of data protection in order to meet the requirements of generally applicable law and to protect the rights of data subjects.

IX. Register of Processing Activities (RPA)

The Controller, from the date the Policy begins, will maintain an appropriate Register of Processing Activities (RPA), including all activities occurring in the reporting abuse process. The RPA will be maintained in a manner that ensures appropriate confidentiality whilst allowing for oversight of the activities taking place and its effective review.

X. Final provisions

In matters not covered herein, the provisions of relevant local law, as well as the laws of the European Union, in particular the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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) and Directive (EU) 2019/1937 (of the European Parliament and of the Council on the protection of persons who report breaches of Union law) shall apply.