# Speak Up Policy

## INTRODUCTION

At Syensqo, we protect our culture of integrity. We strive to uphold strong ethical and regulatory standards at all times, ensuring our actions align with policies, procedures and with our values and actively contribute to the future of a trusted company.

Integrity means fostering an environment in which every person feels confident and comfortable to speak up and raise concerns in good faith when witnessing potential breaches of law, policies, ethics and compliance standards or Syensqo's Code of Business Integrity. It is about being committed to doing the right thing and about generating a respectful, energising and enjoyable work environment that enables us to perform at our best. We also invite third parties who interact with Syensqo to raise concerns when appropriate.

We cannot address and remediate breaches unless we are aware of them.

This policy which is part of the Syensqo Speak up Program describes :

- the principles of confidentiality and anonymity (if legally permitted), when reporting in good faith a concern, an actual or potential breach of law, policies or our Code of Business Integrity;
- the principles of non-retaliation towards people who report breaches of law, policies or our Code of Business Integrity in good faith;
- the procedure for reporting actual or potential breaches of law, policies or our Code of Business Integrity.

This policy is available on the Syensqo's website [https://www.syensqo.com/en/about-us/ethics-and-compliance/code-business-integrity/], and intranet [https://thehub.syensqo.com/en/corporate-news-center/ethics-compliance-useful-links] and may be updated from time to time. It is applicable to each legal entity in the Syensqo Group ("Syensqo"). Each legal entity will be defined as "the Company" for the purpose of this Policy.

This policy, the reporting channels and procedures are compliant with the requirements of applicable local laws.

## 1. SCOPE

### 1.1. Who can use the Syensqo reporting channels?

The Syensqo reporting channels are accessible to all employees (including Syensqo employees, former employees and candidates in a recruitment process, volunteers and trainees) as well as to any other third party (such as applicants, directors, shareholders, self-employed persons, consultants, contractors, suppliers and customers).

### 1.2. Scope and matter types

The following matter types or reporting categories can be used to report any actual or potential breach of law, policies or our Code of Business Integrity, as well as any information about such breaches and attempts to conceal such breaches:

- Accounting, Auditing Matters, Finance and Banking
- Antitrust/Competition
- Bribery/Corruption
- Computer, Email, Internet use and Social Media
- Confidentiality and Misappropriation
- Conflict of Interest
- Data Privacy
- Discrimination
- Diversity and Inclusion
- Embezzlement, Theft, Robbery
- Public Procurement
- Protection of the environmental and Health, or Safety
- Consumer Protection
- Harassment including Retaliation
- HR Matters
- Human Rights violations
- Insider Trading/Securities Violations

- International Trade/Trade Compliance
- Misconduct or Inappropriate Behaviour (deliberate or not)
- Substance Abuse
- Violence or Threat
- Fraud
- Other

A detailed description of each reporting category above is included in Appendix 1.

## 2. Reporting in good faith

Reports must be made in good faith; if you raise a concern about a potential or actual breach of law, policies or the Code of Business Integrity ("the reporting person"), you need to have reasonable grounds to believe that the information is true at the time of reporting.

If the report is not made in good faith or is made with the sole purpose of damaging others, Syensqo or the Company can take appropriate disciplinary and/or judicial actions against the reporting person in line with the applicable local laws.

## 3. Syensqo reporting procedures

If you have any concerns or information about actual or potential breaches, you are encouraged to report it to Syensqo as soon as possible.

If you are a Syensqo employee, you can always reach out to and speak with your line manager or supervisor. Part of his/her job is to listen to your concerns and act on them appropriately.

If you are a Syensqo employee or a third party, you are encouraged to use the Syensqo reporting channels for reporting an actual or potential breach in line with the reporting procedures in this policy.

You can also reach out to any other person within Syensqo who will refer you to the Syensqo reporting channels when appropriate.

### 3.1. Syensqo reporting channels

You can use the following Syensqo reporting channels:

- the Syensqo Ethics Helpline [https://www.syensqo.com/en/about-us/ethics-and-compliance/ethics-helpline]; or
- an email or a phone call to the Regional Compliance Officer or the Chief Compliance Officer.

Your report will be directly addressed and handled by Compliance professionals and every report will be taken seriously and followed up thoroughly.

#### 3.1.1. Syensqo Ethics Helpline

The Syensqo Ethics Helpline is a safe, reliable, and convenient method to report any actual or potential breach as mentioned under section 2.2. The platform is run by an experienced third-party provider and you can trust that this reporting method is easy-to-use and confidential. Compliance officers will follow up on the report once you have submitted it through the Ethics Helpline.

You can report any concerns through the Syensqo Ethics Helpline (see Appendix 2).

It is toll-free and globally available to all Syensqo employees and third parties 24 hours a day, 7 days a week, 365 days a year; you can call anytime from anywhere. You can make a report in 19 languages. No call-tracing or recording devices are used.

You can find more details about the Syensqo Ethics Helpline in Appendix 2.

#### 3.1.2. Chief Compliance Officer and Regional Compliance Officers

You will find the contact details of the Chief Compliance Officer and the Regional Compliance Officers in Appendix 3.

### 3.2. Anonymous reporting

We strongly encourage you to identify yourself, as this is helpful to properly and thoroughly follow up, investigate and address the reports.

However, if you would feel uncomfortable identifying yourself, you may choose to remain anonymous. An anonymous report will be taken just as seriously as a non-anonymous report and will be handled according to the applicable local laws. If you wish to remain anonymous, you can do so by registering your report with the Syensqo Ethics Helpline by clearly choosing that option.

### 3.3. What information should you include in your report?

We encourage you to be as precise as possible and provide as many details as possible when reporting a concern or a breach.

To facilitate the investigation, your report should ideally include the following details (when the relevant information is known to you):

- a detailed description of the reported events;
- a detailed description of how and when the events came to your attention;
- the date and place of the events;
- the names and job positions of the persons involved, or information enabling their identification;
- the names of any witnesses, if any, who may confirm the reported events or provide any additional information;
- whether anyone within Syensqo is aware of the events and whether anyone tried to cover up or hide the existence of such events;
- how the reported events harm or could harm potentially Syensqo;
- your name (unless if your report is anonymous);
- any other information or elements that may help the investigation team.

When you report through the Syensqo Ethics Helpline, these questions will be asked to you through the platform.

## 3.4. How is your report handled by Syensqo?

### 3.4.1. Procedure

1 - Acknowledgment of receipt

You will receive an acknowledgement of receipt of the report within 7 days. Reporting through the Syensqo Ethics Helpline will generate a file number which allows you to easily follow up on the report's progress.

2 - Analysis of the report and follow-up

The Compliance Officer will assess the information provided in your report and, where relevant, analyse the breach(es) reported and check if it is necessary to carry out an in-depth investigation.

The Compliance Officer will communicate with you, ask you for additional information if necessary, provide you feedback and/or follow up on potential new reports.

If you have chosen to remain anonymous, we encourage you to check the Syensqo Ethics Helpline periodically to learn about the status of your report (in progress or closed) or to answer any possible additional questions raised through the Syensqo Ethics Helpline.

3 - Investigation

The Compliance Officer will decide whether a more in depth investigation is needed.

The Compliance Officer will take the lead in the investigation and may be assisted by internal experts and/or external experts as appropriate.

Investigations will be conducted thoroughly with due regard to the principles of (i) confidentiality, (ii) anonymity (if applicable), (iii) objectivity and fairness to all parties involved and (iv) non-retaliation.

4 - Feedback

The Compliance Officer will provide you with appropriate feedback within a reasonable timeframe, not exceeding three months from the date of the acknowledgement of receipt of the report. If the investigation could not be finalised within such time frame, you will receive an update. Feedback will be shared taking into account confidentiality obligations. If you made a report anonymously, we encourage you to periodically check the status of your report on the Syensqo Ethics Helpline.

5 - Investigation report

Following the investigation, the Compliance Officer, if applicable, will prepare a report describing the investigation measures and actions to be taken. The report may be shared with the senior management of Syensqo on a need-to-know basis only.

The final report will include the findings and the actions to be taken:

i. In the event that a breach is substantiated, relevant measures and disciplinary actions may be taken with the aim of remediating the breach and protecting Syensqo
ii. In case the investigation shows that there is insufficient or no evidence of the alleged breach, no further action will be taken. Process improvements may however still be required as well as feedback to the implicated parties

### 3.4.2. Compliance Officers

All reports will be addressed and handled by independent, dedicated and trained compliance professionals. They are part of the Ethics & Compliance department at Syensqo, reporting to the Chief Compliance Officer. They are duly trained to conduct investigations and may, on a "need to" basis, ask assistance from internal or external experts and will treat the report confidentially to the best extent possible.

Syensqo's Board of Directors oversees the Company's Corporate Governance and Ethics & Compliance strategy. The Speak Up Policy has been approved by the

Executive Leadership Team and the Board of Directors, and the Chief Compliance Officer is accountable for its implementation. The Chief Compliance Officer reports annually to the Audit Committee of Syensqo's Board of Directors about the Speak Up Program, trends and data in accordance with the confidentiality obligations.

### 3.5. Record keeping

Syensqo and/or the Company keeps records of all reports received, in compliance with the confidentiality requirements provided in section 5.1 of this policy.

## 4. SPEAK UP PRINCIPLES

This policy is based on the three following key principles: confidentiality, anonymity and non-retaliation.

### 4.1. Confidentiality

Syensqo takes the necessary measures to ensure that reports and information that could reveal your identity remain confidential and are only disclosed on a need-to-know basis or if foreseen by local laws. Other information also remains confidential and can only be shared on a need-to-know basis.

### 4.2. Anonymity

Anonymity of the reporting person is explained under section 4.2.

### 4.3. Protection against retaliation

Regardless of how you report a breach, you are protected from any form of retaliation. Any person mentioned in section 2.1, who reports a breach of law, policies and the Code of Business Integrity in good faith according to this policy will be protected against retaliation under the Syensqo Speak Up Program.

Any person, regardless of position, who engages in retaliatory behaviour will be subject to disciplinary or judicial actions in accordance with the applicable local laws.

## 5. Provisions applicable to EU countries only

### 5.1. Compliance with EU law and local laws

This policy and the aforementioned reporting channels and procedures are compliant with the requirements of the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union Law (The Directive) and applicable local laws.

### 5.2. Scope

Although the EU law and local laws might be more restrictive, the Syensqo reporting channels allow reporting on actual or potential breaches of all matters mentioned in section 2.2.

### 5.3. Syensqo reporting channels

See section 3.4.1. (Syensqo Ethics Helpline) and 3.4.2 (Compliance Officers).

It is recommended to use the Syensqo reporting channels mentioned under section 4.1 to make a report. For Belgium, Italy and France: if you would nevertheless feel uncomfortable using the Syensqo reporting channels mentioned under section 4.1, it is also possible to report via the local point of contact (the "local Whistleblowing Officer").

#### 5.3.1. Local reporting channels

You can use the following channels:

- a face-to-face meeting with the local Whistleblowing Officer;
- an e-mail to the local Whistleblowing Officer.

The contact information of the local Whistleblowing Officers are available in Appendix 4.

### 5.3.2. Anonymous reporting

For anonymous reporting, we encourage you to use the Syensqo Ethics Helpline. A specific feature in the Helpline is installed to enable making anonymous reports in a very easy and accessible way.

If you nevertheless feel uncomfortable using the Syensqo Ethics Helpline and you still wish to report anonymously for Belgium, Italy and France, you can address an email to the local Whistleblowing Officer, through an email provider (Outlook, Gmail etc.), from which your identity cannot be deducted.

## 5.4. Procedure

See section 3.4.1.

We strongly encourage you to use the Syensqo reporting channels mentioned under section 4.1. as your report will be handled by independent, dedicated and trained Ethics & Compliance professionals. If you nevertheless feel uncomfortable, you can reach out to the local Whistleblowing Officer and the following procedure will apply.

You will receive an acknowledgement of receipt of the report within 7 days of the receipt. The local Whistleblowing Officer will assess the information provided in your report and will communicate with you, ask you for additional information if necessary, provide you feedback and follow up on potential new reports. The local Whistleblowing Officer consults with the Compliance Officer to conduct an investigation. The local Whistleblowing Officer will provide you appropriate feedback within a reasonable timeframe, not exceeding three months from the date of the acknowledgement of receipt of the report. If the investigation could not be finalised, you will receive an update. Feedback will be shared taking into account confidentiality obligations.

## 5.5. Confidentiality and protection against retaliation

Confidentiality and the protection against retaliation under the EU law and the local laws of EU countries are only applicable for reports related to breaches as foreseen

by local laws. Syensqo will comply with additional protective measures foreseen in the local laws of EU countries, if needed.

### 5.6. External reporting channels

You can use an external reporting channel after having first reported through the Syensqo reporting channels or can go directly through the external reporting channels if you consider it more appropriate. Be aware that external reporting channels outside of Syensqo can only be used for reports related to breaches regarding well-defined matters. More information about these external reporting channels can be found in Appendix 5.

## 6. PROCESSING OF PERSONAL DATA

In the framework of the internal reporting procedures, the Company is considered as a joint data controller for the processing of personal data together with Syensqo.

In this framework, personal data may also be communicated to external service providers, in particular to Navex, i.e. the provider in charge of the platform for the Syensqo Ethics Helpline, who will act as data processor.

Any processing of personal data carried out pursuant to this policy will be carried out in accordance with the applicable personal data protection laws, including the European General Data Protection Regulation ("GDPR") and local data protection laws.

The following personal data may be processed in the context of a report: your name, function, start date of collaboration (if applicable), contact information and e-mail address unless the report is done anonymously, and of persons, involved in the breach, any identified or identifiable information provided by you and collected in the context of the internal investigation. This processing of data is done in the context of complying with a legal obligation and/or the legitimate interest of the Company, to the extent that the internal reporting channel exceeds legal objectives, in particular the detection of breaches, ensuring the security and ethical conduct of the Company and/or Syensqo.

Personal data which are manifestly not relevant for the handling of a report shall not be collected or, if accidently collected, shall be deleted without undue delay. Relevant data will be kept until the breach reported is expired and in any case for a period of five years after the report.

These data can also be transmitted outside the European Economic Area and/or be accessed from countries outside the European Economic Area to Syensqo's entities and to our subcontractors involved in the process. Syensqo has taken the appropriate safeguards to ensure the security of the data. You may request additional information in this respect and obtain a copy of the applied safeguard by exercising your rights as set out below.

All individuals whose personal data are processed in the context of reports of breaches have, within the applicable legal conditions, the right to access and copy, right to rectification, right to data erasure (providing that there is no limitation from a legal obligation), right to object (unless the legal basis is a legal obligation), right to limit the processing activity and the right to lodge a complaint with the supervisory authority in accordance with applicable law. However, these rights may be limited by the rights and freedoms of others, in particular the reporting person's right to confidentiality and the Company's right to follow-up on the report properly.

For more information on the processing of personal data,please refer to the Navex Privacy Notice and Syensqo Privacy Policy (attached in Appendix 6).

## 7. ENTRY INTO FORCE

This policy is effective from January 1st, 2024 for an indefinite period.

Syensqo may amend this policy at any time, including but not limited to changes in relevant legislation and/or operational needs.

Appendices:

- Appendix 1: Speak Up matters and their description
- Appendix 2: Ethics Helpline
- Appendix 3: Chief Compliance Officer and Regional Compliance Officers
- Appendix 4: Local Whistleblowing Officers

- Appendix 5: External Reporting Channels
- Appendix 6: Privacy Notice and Privacy Policy

## Appendix 1 Speak up matters and their description

| Matter type | Description |
|---|---|
| Accounting, Auditing Matters, Finance and Banking | The unethical systematic recording, analysis of the business and financial transactions associated with generally accepted accounting practices and concerns regarding questionable or unethical banking practices. (Examples include: misstatement of revenues, misstatement of expenses, and misstatement of assets, misapplications of GAAP principles, wrongful transactions, money laundering, bank fraud; embezzlement; altering, fabricating, falsifying or forging of any banking document, report or record). |
| Antitrust/Competition | Oral or written agreements, arrangements or understandings with other business parties to fix prices; boycott specific suppliers or customers; allocate products, territories or markets; or exchange competitively sensitive information; as well as discussions regarding price, trade allowances or rebates, costs, competition, marketing plans or studies, production plans and capabilities or any other confidential information. |
| Bribery/Corruption | The act of influencing the action of another (private or public party) by offering or promising some advantage (favors, payments, gifts, entertainment) that could be reasonably interpreted as an effort to improperly influence a decision. |
| Computer, Email, Internet use and Social Media | Unauthorized or inappropriate use of any Company computer system, emails or internet including references to the company or its employees through any social media. |

| | |
|---|---|
| Confidentiality and Misappropriation | Confidentiality refers to the protection of the Company's and our customer's non-public information and use of such information only for legitimate business purposes. Misappropriation refers to the unauthorized or improper use of a third party's intellectual property rights, including patents, trademarks, copyrights and trade secrets. |
| Conflict of Interest | A conflict of interest is defined as a situation in which a person, such as a public official, an employee, or a professional, has a private or personal interest sufficient to appear to influence the objective exercise of his or her official or professional duties. (Examples include: inappropriate vendor relations, bribery, inappropriate customer relations). |
| Consumer Protection | Refers to the practice of safeguarding the end-user consumer of goods and services against unfair commercial practices in the marketplace. |
| Data Privacy | Breach of the duty to guard, protect and process personal information in compliance with the law and current policies. |
| Discrimination | Employment decisions/treatment based on protected categories such as race, color, religion, national origin, age, disability, gender, and other protected categories. |
| Diversity and Inclusion Matters | Any type of discrimination or non-inclusive behavior toward an individual or group due to their representation of various identities and differences. |
| Embezzlement, Theft, Robbery | Embezzlement - To appropriate (as property entrusted to one's care) fraudulently to one's own use. (Examples include: bookkeeping errors, misapplication of funds, and mishandling of cash). |

| | |
|---|---|
| | Robbery - the crime of stealing from somewhere or someone.<br><br>Theft - The act of stealing; specifically: the felonious taking and removing of personal property with intent to deprive the rightful owner of it. |
| Environmental, Health, or Safety | Violation of any environmental law, regulation, corporate policy or procedure with respect to the handling and disposal of hazardous materials or the health and safety of other individuals. |
| Fraud | Any matter related to fraud that is not listed above including social and tax fraud. |
| Harassment including Retaliation | Harassment is any conduct with the purpose or effect of violating the dignity of a person or creating an intimidating, hostile, degrading, humiliating, bullying, or offensive work environment, including moral or sexual harassment.<br><br>Retaliation for making a complaint/report or for participating in an investigation or legal proceeding related to any potential violation of policy or law. |
| HR Matters | HR matters include compensation, benefits, recruitment, firing as long as they do not involve potential criminal or administrative violations. |
| Human Rights violations | Actions, omissions, activities, policies, or practices that infringe on Human Rights in violation of law or company policies. Prohibited conduct includes, but is not limited to, forced labor, child labor, human trafficking, abuse of immigrant workers or undocumented migrants. |
| Insider Trading/Securities Violations | Infringement, transgression; specifically: an infringement of the rules which securities acts define or internal police. |

| | |
|---|---|
| International Trade/Trade Compliance | Violation of any import or export law, corporate policy or procedure regarding export control (dual use /military), trade control (chemical precursors, dangerous chemicals, etc.) and economic sanctions. Examples include, transactions involving an embargoed country, a sanctioned entity and export of products or transfer of technology without appropriate licenses in place. |
| Misconduct or Inappropriate Behaviour (deliberate or not) | Intentional wrongdoing; specifically: deliberate violation of a law or standard. |
| Substance Abuse | Substance abuse is defined as the misuse of both legal and illegal drugs including alcohol. (Examples include: cocaine, narcotics, marijuana, stimulants) |
| Public Procurement | Refers to the rules of procedure for the award of certain works contracts, supply contracts, services contracts, and concessions, by government, authorities and state-owned enterprises operating notably in the fields of defence, security, water, energy, transport and postal services. |
| Violence or Threat | Violence is an expression of the intention to inflict evil, injury, or damage to a person or their property. (Examples include: direct, veiled, conditional, violent) |
| Other | Any matter type of public interest that has not been identified in the list above, e.g. criminal offences, any violation of applicable EU law or local laws. |

## Appendix 2 Ethics Helpline

### 1. Making a Report by Phone

The telephone service is available in all countries where Syensqo operates.

### 1.1. Direct call

The countries below have a direct contact number. In these cases, there are no additional steps you need to take, just dial the phone number corresponding to your country:

| COUNTRIES | NUMBERS | COUNTRIES | NUMBERS |
|---|---|---|---|
| Argentina | 0800-345-2407 | Malaysia | 1800-81-0817 |
| Australia | 1800 292 034 | Mexico | 8008801713 |
| Austria | 0800 298905 | Netherlands | 0800 2500106 |
| Belgium | 0800 13 331 | New Zealand | 0800 870 017 |
| Brazil | 0800 762 0026 | Norway | 800 62 682 |
| Canada | 844-486-1664 | Peru | 0800 74873 |
| Colombia | 01-800-5189515 | Poland | 800 005 353 |
| Chile | 800 914 559 | Portugal | 800 815 091 |
| Czech Republic | 800 810 255 | Romania | 0800 890 549 |
| Croatia | 0800 988 956 | Saudi Arabia | 800 850 1648 |
| Denmark | 80 83 10 22 | Serbia | 0800 800629 |
| Finland | 0800 418633 | Singapore | 800 492 2779 |
| France | 0800 90 52 32 | South Africa | 080 001 0745 |
| Germany | 0800 181 4739 | South Korea | 080-870-3137 |
| Greece | 800 600 0682 | Spain | 900 751 412 |
| Guatemala (Claro) | 999-9190 | Sweden | 020 79 54 49 |
| Hong Kong | 800 902 154 | Switzerland | 0800 000 520 |
| Hungary | 06 80 020 152 | Taiwan | 00801-49-1248 |
| India | 022 5097 2946 | Thailand | 1800 018 160 |
| Indonesia | 021 50918409 | Turkey | 800 492 408 801 04 |
| Ireland | 1800 849 248 | United Arab Emirates | 800 012 025 5 |
| Italy | 800 819 531 | United Kingdom | 0 800 066 8124 |
| Jamaica | 1 (876) 677-9169 | Uruguay | 0 004 05 423 6 |
| Japan | 0800-600-8387 | USA | 844-486-1664 |
| Kazakhstan | 8 (800) 080-82-85 | Venezuela | (English) 0-800-225-5288 (Spanish) 0-800-552-6288 |

| | | | |
|---|---|---|---|
| Latvia | 80 000 101 | Vietnam | 024 4458 1809 |
| Luxembourg | 800 25 132 | | |

### 1.2. Other countries

For the countries below there is no phone number available. Please make your report using one of the other channels available listed above.

- Congo (Democratic Republic of Congo);
- Mongolia;
- Morocco;
- Ukraine;
- Zambia.

## 2. Making a report online

You can make a report online:

- by accessing the web intake site's URL [syensqo.ethicspoint.com] using a computer;
- by using a mobile phone and
  (i) accessing the web intake site's URL [https://syensqo.navexone.eu], or
  (ii) scanning the QR Code:

## Appendix 3 Chief Compliance Officer and Regional Compliance Officers

| | |
|---|---|
| Chief Compliance Officer | Name: Véronique Roedolf<br>Tel. nº: +32 471 62 50 53<br>Email address:<br>veronique.roedolf@syensqo.com |

| **Geographical scope** | **Regional Compliance Officers** |
|---|---|
| APAC | Name: Shammann Miao<br>Tel. nº: +86 21 2350 1226<br>Email address:<br>shammann.miao@syensqo.com |
| EMEA | Name: Elsa Odjet<br>Tel. nº: +33 4 2619 7081<br>Email address: elsa.odjet@syensqo.com |
| NAM-LATAM | Name: Rachel Wiemer<br>Tel. nº: +1 (609) 480-0061<br>Email address:<br>rachel.wiemer@syensqo.com |

## Appendix 4 Local Whistleblowing Officers

| EU country | Local Whistleblowing Officers |
|---|---|
| Belgium | Name: Werner Engel<br>Tel. n°: +3 249 7231377<br>Email address: werner.engel@syensqo.com |
| France | Name: Elsa Odjet<br>Tel. n°: +33 4 2619 7081<br>Email address: elsa.odjet@syensqo.com |
| Italy | Name: Anna Calderini<br>Tel. n°: +39 0229092171<br>Email address:<br>anna.calderini@syensqo.com |

## Appendix 5 External reporting channels

This appendix includes the external reporting channels available in each European country where Syensqo operates.

European Agencies:
• European Anti-Fraud Office (OLAF) Report fraud: https://european-union.europa.eu/index_en
• European Maritime Safety Agency (EMSA): http://www.emsa.europa.eu/
• European Aviation Safety Agency (EASA): https://www.easa.europa.eu/confidential-safety-reporting
• European Security and Markets Authority (ESMA): https://www.esma.europa.eu/investor-corner/make-complaint
• European Medicines Agency (EMA): https://www.ema.europa.eu/en/about-us/contacts-european-medicines-agency#report-an-issue-with-an-authorised-product-section
• European Commission How to make a complaint at EU level | European Commission (https://commission.europa.eu/about-european-commission/contact/problems-and-complaints/complaints-about-breaches-eu-law-member-states/how-make-complaint-eu-level_en)

| EU country | External reporting channels |
|---|---|
| Austria | Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung<br>• (BMI-III-BAK- SPOC@bak.gv.at): https://www.bak.gv.at/601/ or https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=8HObc4&c=-<br>• Finanzmarktausicht FMA https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=11FMA61&c=-<br>• Gelwäschemeldestelle https://www.bundeskriminalamt.at/308/start.aspx |
| Belgium | Federal Coordinator's contact details are as follows:<br>• Address: Leuvenseweg 48 bus 6, 1000 Brussels<br>• Email: integrity@federalombudsman.be<br>• Telephone: 02 289 27 04<br>• Online reporting: |

| | |
|---|---|
| | ○ French site – médiateur fédéral: https://www.federaalombudsman.be/fr/centre-integrite/signalez-une-atteinte-a-lintegrite-ou-une-violation-de-la-legislation<br>○ English site – federal ombudsman: https://www.federaalombudsman.be/en/whistleblowers/reporting-integrity-violations-or-breaches-of-law<br>○ Dutch site – federale ombudsman: https://www.federaalombudsman.be/nl/klokkenluiders/meld-een-integriteitsschending-of-inbreuk-op-de-wetgeving<br>○ German site – föderale Ombudsmann: https://www.federaalombudsman.be/de/whistleblowers/melden-sie-eine-verletzung-der-integritat-oder-einen-rechtsverstoss |
| Croatia | Croatian Ombudsman:<br>• https://www.ombudsman.hr |
| Czech Republic | Czech Ministry of Justice:<br>• https://oznamovatel.justice.cz/chci-podat-oznameni/ |
| France | • Defender of right: Orientation et protection des lanceurs d'alerte \| Défenseur des Droits: https://defenseurdesdroits.fr;<br>• Specific administrative authorities depending on the area concerned (see complete list of the administrative authorities annexed to the French Decree No.2022-1284 of October 3, 2022).<br>• Défenseur des Droits: https://www.defenseurdesdroits.fr/<br>• Agence française anticorruption (AFA): https://www.agence-francaise-anticorruption.gouv.fr/fr/faire-signalement<br>• Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF): https://www.economie.gouv.fr/dgccrf<br>• Autorité de la concurrence: https://www.autoritedelaconcurrence.fr/fr<br>• Autorité des marchés financiers (AMF): https://www.amf-france.org/fr/formulaires-et-declarations/lanceur-dalerte-0<br>• Autorité de contrôle prudentiel et de résolution (ACPR): https://acpr.banque-france.fr/<br>• Inspection générale de l'environnement et du développement durable (IGEDD): https://www.igedd.developpement-durable.gouv.fr/<br>• Commission nationale de l'informatique et des libertés (CNIL): https://www.cnil.fr/fr<br>• Agence nationale de la sécurité des systèmes d'information (ANSSI): https://www.ssi.gouv.fr/ |

| | |
|---|---|
| | • Direction générale des finances publiques (DGFIP): https://www.economie.gouv.fr/dgfip<br>• Direction générale du travail (DGT): https://travail-emploi.gouv.fr/<br>• Délégation générale à l'emploi et à la formation professionnelle (DGEFP): https://travail-emploi.gouv.fr/<br>• Direction générale des douanes et droits indirects (DGDDI): https://www.douane.gouv.fr/<br>• Service central des armes et explosifs (SCAE): https://www.interieur.gouv.fr/<br>• Contrôle général des armées (CGA): https://www.defense.gouv.fr/cga<br>• Collège des inspecteurs généraux des armées: https://www.defense.gouv.fr/ |
| Germany | • External Federal Reporting Office as part of the Federal Ministry of Justice: https://www.bundesjustizamt.de/DE/MeldestelledesBundes/MeldestelledesBundes.html<br>• German Federal Cartel Office in the event of violations of the law against restraints of competition: https://www.bundesjustizamt.de/DE/MeldestelledesBundes/MeldestelledesBundes.html<br>• Federal Financial Supervisory Authority in the event of violations of the financial services supervision act: https://www.bafin.de/DE/DieBaFin/Hinweisgeberstelle/hinweisgeberstelle_node.html |
| Ireland | • Protected Disclosures Commissioner https://www.opdc.ie/<br>• Protected Disclosures (Whistleblowing): List of prescribed persons https://www.gov.ie/en/collection/41798-protected-disclosures-whistleblowing-list-of-prescribed-persons/<br>• See also: https://www.citizensinformation.ie/en/employment/enforcement-and-redress/protection-for-whistleblowers/#l3ea3f |
| Italy | • National Anti-Corruption Authority: Autorità Nazionale Anticorruzione: https://www.anticorruzione.it/-/whistleblowing |
| Netherlands | • Huis voor Klokkenluiders https://www.huisvoorklokkenluiders.nl/<br>• Autoriteit Consument & Markt (ACM): https://www.acm.nl/nl/contact/tips-en-meldingen/bescherming-klokkenluiders<br>• Autoriteit Financiële Markten (AFM) https://www.afm.nl/nl-nl/sector<br>• Autoriteit Persoonsgegevens (AP) https://autoriteitpersoonsgegevens.nl/en<br>• De Nederlandsche Bank N.V. https://www.dnb.nl/<br>• Inspectie Gezondheidszorg en Jeugd (IGJ) https://www.igj.nl/b<br>• De Nederlandse Zorgautoriteit (NZa) https://www.nza.nl/ |

| | |
|---|---|
| Portugal | • Ministério Público: https://dciap.ministeriopublico.pt/perguntas-frequentes/apresentar-denuncia and https://www.ministeriopublico.pt/perguntas-frequentes/queixa;<br>• Polícia Judiciária: https://www.policiajudiciaria.pt/denuncia-anonima/ and https://www.policiajudiciaria.pt/ under Comunicações Communicacoes/queixa eletrónica<br>• Polícia de Segurança Pública and Guarda Nacional Republicana https://queixaselectronicas.mai.gov.pt/<br>• Banco de Portugal; Participate in a \| Bank of Portugal (https://www.bportugal.pt/) |
| Romania | The National Integrity Agency (Agentia Nationala de Integritate):<br>• Online: https://avertizori.integritate.eu/<br>• Email: avertizari@integritate.eu |

## Appendix 6 Privacy notice and privacy policy

### 6.1. Navex Privacy Notice

DATA PRIVACY NOTICE AND CONSENT

The data privacy regulations of some countries require that a person making a report containing personal data must be notified of certain collection and retention practices regarding information submitted through this system, as well as consent to certain terms and conditions regarding the information submitted by that person. Because you have indicated that you either live in or are reporting about a matter that occurred in a country with such regulations, you are being asked to read and accept the terms contained in the Consent below. If you do not wish to accept the terms below, we are unable to accept any information through this system and would ask that you please report this matter to your local Management, Human Resources, the Law Department or Regional Compliance Officer instead.

The Syensqo Ethics Helpline site is a confidential online reporting system operated by EthicsPoint and provided by Syensqo to allow you to ask questions and to report incidents. Use of the Syensqo Ethics Helpline site is entirely voluntary. You are encouraged to follow our existing internal reporting processes, but if you feel that you are unable to do so, you may use the Syensqo Ethics Helpline to do so. If your concern pertains to issues not listed, you are encouraged to report them to local management or through our other established reporting channels.

Before proceeding further, please read the notice below and, if you agree, check the consent box that follows. You will then be able to submit a report or question on the Syensqo Ethics Helpline site. If you do not provide your consent, you will not be able to submit a report or question.

Please be aware that the information you supply about yourself, your colleagues, or any aspect of the company's operations may result in decisions that affect others. Therefore, we ask that you only provide information that, to the best of your knowledge, is correct and factual. While you will not be sanctioned for submitting information in good faith, even if it later turns out to be incorrect, knowingly providing false or misleading information will not be tolerated. The information you submit will be treated confidentially and we encourage you to identify yourself in order for us to follow up with questions we may have.

<u>What Information is collected?</u>

The Syensqo Ethics Helpline captures the following information: your name and contact details, any question you may have, the name and title of all individuals you may be reporting, and a description of any questionable conduct, including all relevant details.

How will the Information be used?

The information you provide will be stored on servers hosted by EthicsPoint, Inc. in Frankfurt, Germany ("EthicsPoint"). As EthicsPoint is an American company, Syensqo has entered into a data processing agreement ("DPA") providing data protection guarantees equivalent to those set out in European legislation ("GDPR"). Unless otherwise required by law, the information within the Syensqo Ethics Helpline database may only be reviewed and used by those individuals who need to access the data to fulfill their job duties. These individuals are the Syensqo's compliance officers, the Syensqo Group General Counsel and the technical staff at EthicsPoint. Those individuals may be located in the United States. In addition, all information you provide may be stored by Syensqo in the course of answering your question(s) or investigating the report.
Syensqo will evaluate the information you provide, and may conduct an investigation and/or take corrective action.

Please note that because of applicable laws, individuals you identify through the Syensqo Ethics Helpline site may be informed about the fact that a report has been made. However, the information you provide will not reveal your name or identity. In addition, all such individuals you identify will have the right to respond to or correct information you reported.
Any information you submit that is not needed to answer your question or for the investigation of any incident will be deleted or archived, as permitted by local law. In addition, once we have responded to your question or completed any investigation, all information you submitted will be deleted or archived, as appropriate and permitted by local law. Syensqo will take adequate technical, organisational, and legal steps to secure the information you provide. Syensqo also requires EthicsPoint to adequately secure your personal data and not use it for any unauthorised purposes. (See the EthicsPoint, Inc. Privacy Policy for additional information: http://www.ethicspoint.com/privacy-policy/).

The process of submitting a report via the website [http://syensqo.ethicspoint.com], includes the acknowledgment of the "Information notice regarding whistleblowing".
For more information on the Navex Privacy Statement please consult the website [https://www.navex.com], available at the bottom of the webpage.

### 6.2. Syensqo Data Protection Policy

You can consult at any time the applicable Syensqo Data Protection Policy, Privacy Policy and Cookie Policy always available in the "Privacy & Cookie Policy" section at www.syensqo.com.
For more information about the processing of your personal data, you can contact the Syensqo Data Protection & Privacy Office as specified in the above policies.

As of 01/01/2024

* 10/12/2024: Revision of section '3.4.2 Compliance Officers' for clarification in line with CSRD requirements.