PROCEDURE RELATING TO THE WHISTLEBLOWING MECHANISM
Plastic Omnium Group

In accordance with the provisions of the Code of Conduct, the Plastic Omnium Group, defined as including any entity controlled by Compagnie Plastic Omnium in all countries (hereinafter referred to as the "**Group**" or "**Plastic Omnium**"), has set up a whistleblowing mechanism (hereinafter the "**Mechanism**"). This dedicated Mechanism enables the Group's corporate officers, former or current employees, interns, seconded, temporary workers, candidates for employment, shareholders and other individuals, and all its stakeholders such as contractors, suppliers, subcontractors, customers, and their employees (together the "**Reporters**"), to report any irregularity within the scope of the Mechanism. Reporters using this Mechanism with good faith will usually be referred to as "**Whistleblower(s)**".

Full information regarding use of the Mechanism is set out below. **This document can be viewed by employees on the Group's intranet site or will be provided to them by any means before they start working within the Group. For external stakeholders, it can also be viewed on the Plastic Omnium Group's website.**

Use of the Mechanism is optional and no sanction will be incurred for failure to use the Mechanism to report conduct, a grievance or an alleged offence within its scope.

Plastic Omnium operates as one business and it is important that we apply common values and show high levels of integrity globally, throughout the Group. As such, this procedure will apply across all offices. However, we are mindful that nuances exist in local legislation that will need to be observed, and so you will find Local Addendum appended to this procedure. The Local Addendum only includes local specificities when those differ significantly from the global procedure, and do not aim to replace the global procedure.

The scope of the Mechanism

This Mechanism enables Whistleblowers to report information relating to:

- ✓ a crime or other infringement of criminal law or any other offence, including administrative;
- ✓ a breach or attempt to conceal a breach of (i) an international obligation duly ratified or approved in the relevant country of the Whistleblower , (ii) a unilateral commitment of an international organisation given on the basis of a duly ratified international obligation, (iii) European law, (iv) the law or regulations;
- ✓ a threat or harm to the public interest;
- ✓ the existence of conduct or situations contrary to the Group's Code of Conduct, insofar as they are likely to constitute acts of corruption or influence peddling;
- ✓ a risk to, or serious infringement of, human rights and fundamental freedoms, the health and safety of persons or the environment, resulting from the Group's activities or those of the companies under its control, or from the activities of subcontractors or suppliers with which established commercial relationships exist, when those activities are

connected to such relationships.

Note, however, that reports cannot relate to matters covered by the secrecy of national security information, doctor-patient confidentiality, legal professional privilege the secrecy of a criminal investigation or judicial deliberations.

The functioning of the Mechanism

1. Triggering the Mechanism

In the event that a breach is detected in the areas referred to in the above paragraph, Reporters may first discuss it with their direct and immediate manager, or with that person's manager. If discussing the matter with their manager or with that person's manager might present difficulties, there are other ways for Reporters to make their report.

Whistleblowers can submit an alert by telephone or web through EthicsPoint from Navex using the contact details below. This independent service is available 24/7.

plasticomnium.ethicspoint.com

Telephone numbers are listed in the Local Addendum.

Videoconference or in-person meetings can also be arranged, if requested by the Whistleblower. The meeting will take place within a reasonable amount of time and in any event no later than 20 days following that request.

Whistleblowers are encouraged not to use the Mechanism anonymously. Exceptionally, reports made by persons wishing to remain anonymous can be dealt with, but only if the seriousness of the facts mentioned is established and the factual information is sufficiently detailed. If a Whistleblower has requested to remain anonymous, unless otherwise required by law or with the consent of such Whistleblower, the Group will refrain from any attempt to reidentify the Whistleblower. In addition, any further exchange with the Whistleblower will be carried out while preserving this anonymity. For instance, the Whistleblower may be asked to provide an e-mail or postal address that does not enable him/her to be reidentified.

Whistleblowers must:

- ✓ act in good faith;
- ✓ rely only on information formulated in an objective manner, falling within the scope of the Mechanism; and
- ✓ attach to the form any document or information likely to prove the facts alleged.

Once the report has been submitted, the Whistleblower will be provided with an acknowledgement of receipt within seven days following receipt of the alert, in writing via EthicsPoint

Reporters may also submit an alert to European bodies and institutions or to the competent national authority directly. Competent authorities may vary from one jurisdiction to another. More information about competent authorities per jurisdiction and procedures for reporting

externally can be found in the Local Addendum.

2. The processing of reports

The procedure for verifying the admissibility of reports

Plastic Omnium has set up an ad hoc committee composed of the Group HR VP, Group Compliance and the Head of Internal Audit to assess the admissibility of the alerts (the "**Ad Hoc Committee**").

Plastic Omnium reserves the right to discard alerts that do not meet conditions defined by applicable laws, and in such situations, it will inform the Whistleblower and specify why the alert does not meet legal requirements. In this case the alert may be forwarded to another department for appropriate handling outside of this procedure.

The information associated with the report will be destroyed immediately or archived without delay in anonymous form.

If the report is admissible, it will then be processed and an investigation carried out.

The investigation

The report will be investigated by one or several persons appointed by the Ad Hoc Committee, either at group or local level (the "**Investigator**" or "**Investigators**"). The Investigator may be assisted by people from other departments or by external services providers, if needed. Alerts received by other functions through other channels (i) must be immediately redirected to the Compliance Function and (ii) all information relating to these alerts must be then deleted by the non-autorised person(s).

In the exercise of his or her investigatory functions, the Investigator guarantees:

- ✓ that all data and information received and used in the context of his or her investigatory mission will remain confidential, especially the identity of the Whistleblower, of the person subject to the alert, as well as of any third parties mentioned in the alert – access to this information by non-authorized staff is strictly forbidden and could lead to disciplinary sanctions and in some countries to criminal sanctions;
- ✓ that he or she will communicate appropriately with those who have a legitimate need to know about the investigation while maintaining confidentiality and security of sensitive or personal information, as required by applicable laws and regulations; and
- ✓ that any data, information or document on the basis of which he or she is required to take action will be exhaustively analysed.

Both the Whistleblower and the Investigator will have the possibility to upload messages to each other through EthicsPoint or, if the Whistleblower has agreed to share his/her identity, through direct means of communication. Follow-up and feedback to the Whistleblower should

take place within a reasonable timeframe that must not exceed three months. The Reporter will be informed of the closure of the investigation.

The guarantees provided

1. The confidentiality of the Whistleblower's identity

The Group will ensure that the confidentiality of the Whistleblower's identity is strictly observed. Any information that may reveal the identity of the Whistleblower cannot be disclosed without his or her consent, except to the court. In that case, the Whistleblower will be informed unless such information would jeopardize the related judicial proceedings.

All persons assisting the Investigator in the context of the Mechanism must observe the strictest confidentiality with regard to such information, and particularly information relating to the Whistleblower's identity, as well as those of third parties mentioned in the alert.

2. The absence of sanctions

Whistleblowers acting in good faith cannot be dismissed, sanctioned or discriminated against in any way for having reported facts in accordance with the Mechanism, even if those facts prove to be incorrect thereafter or do not result in any action being taken.

Conversely, abuse of the Mechanism, if proven, could result in disciplinary and, depending on the factual circumstances and applicable laws, legal action, being taken against the Whistleblower.

3. The absence of retaliation

The Group will not tolerate retaliation, including threats or attempts of retaliation, against Whistleblowers. Protection against retaliation also apply to persons who assisted Reporters in the submission of the alert (including non-profitable legal entities such as NGOs or trade unions), individuals who have a professional or personal relationship with the Reporter (e.g., a colleague) and who may be targeted by retaliation measures because of their relationship to the Reporter, a corporate entity with a professional tie with the Reporter (e.g., an entity that is owned by the Reporter, or that employs the Reporter) (together "**Protected Third-Parties**").

4. The gathering of personal information and its retention period

The gathering of personal information

In the context of the Mechanism, the collection and processing of personal data by the Group will be carried out in compliance with EU General Data Protection Regulation 2016/679 of 27 April 2016 (the "**GDPR**"), French Law no.78/17 of 6 January 1978 and its application decree no.2019-536 of 29 May 2019 (the "**French LIL**") (together, the "**Data Protection Laws**"), as well as the CNIL's guidance on whistleblowing systems dated 6 July 2023 (the "**CNIL Guidance**").

The receipt of a report gives rise to data processing managed by one of the Group's subsidiaries, Plastic Omnium Gestion, whose registered office is at 19 boulevard Jules Carteret, 69007 Lyon, acting as an independent controller.

A data protection impact assessment will be carried out by the Group and the Data Protection Officer will be consulted prior to carrying out the processing activities under the Mechanism, in accordance with Data Protection Laws.

In the context of a report, only the following categories of information can be recorded:

- ✓ the identity, functions and professional contact details of the Whistleblower (except in the case of an anonymous report);
- ✓ the identity, functions and professional contact details of persons subject to a report;
- ✓ the identity, functions and professional contact details of persons involved in the reception and/or processing of a report;
- ✓ the identity, functions and professional contact details of the person(s) consulted or heard in the gathering or treatment of the report;
- ✓ the facts reported;
- ✓ the evidence gathered in the context of verification of the facts reported;
- ✓ the report on verification/investigation operations;
- ✓ the actions taken in response to the report.

Once the controller took the decision after the investigations are completed, only the data necessary for the following purposes can be kept:

- ✓ ensuring the protection of the different data subjects (Whistleblower, facilitators, data subject mentioned or subject of the alert) against retaliation ;
- ✓ allow the establishment, exercise or defence of legal claims ;
- ✓ perform internal or external audits of its compliance procedures.

In addition:

- ✓ only personal data that is relevant, adequate and not considered excessive is collected, in accordance with Data Protection Laws;
- ✓ the use of personal data is strictly limited to the treatment and investigation of the alerts and personal data processed in relation to the alerts can not be reused for any

other purposes incompatible with the purpose for which personal data was initially collected;

- ✓ the processing activities carried out in relation to the treatment of alerts will be included in the Group's record of data processing activities; and
- ✓ after having ensured the necessity and relevance of the personal data it uses, the Group will also ensure the quality of the personal data it processes throughout the processing activity (in particular that the personal data is accurate and up to date).

In the context of this processing, the collection of sensitive data (*i.e.* personal data revealing a person's ethnic or supposedly racial origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, data concerning health, or data concerning the sex life or sexual orientation of an individual) ("**Sensitive Data**"), may only be carried out insofar as the implementation of the Mechanism:

- ✓ meets an important public interest (within the meaning of Article 9.2.g) of the GDPR); or
- ✓ is necessary, where applicable, for the establishment, exercise or defense of legal claims (within the meaning of Article 9.2.f) of the GDPR).

Personal data relating to offences (*i.e*. offences, convictions and security measures) ("**Criminal Data**") may only been collected and processed under the conditions set out in article 10 of the GDPR and article 46 of the French LIL.

In addition, the processing of Sensitive Data and Criminal Data may be carried out:

- ✓ if authorized by specific provisions of French law (for example, articles 8 or 17 of the "Sapin 2" law, article L. 225-102-4.-I. of the French Commercial Code, etc.); or
- ✓ to enable the data controller to "*prepare and, where appropriate, bring and pursue legal action as victim, respondent or on their behalf*", in accordance with article 46-3° of the French LIL.

The Group may outsource all or part of the procedure for the processing of reports, while ensuring that subcontractors observe any security measures necessary to preserve the confidentiality of the information.

The Group will not transfer any personal information gathered and processed in the context of the Mechanism outside the European Union. Any transfer of personal information to a third country will be subject to the appropriate guarantees in accordance with the Data Protection Laws, and the persons concerned will be informed.

The Whistleblower can make a complaint to the French Data Protection Authority (the "**CNIL**") with regard to any matter relating to the processing of personal information managed by the Group in the context of the Mechanism.

🕓 *The period of retention of personal information*

Information relating to a report considered by the Investigator as not within the scope of the Mechanism will be destroyed or archived without delay in anonymous form.

If, after investigation, the whistleblowing report is not substantiated, and does not give rise to any disciplinary or legal proceedings, personal information relating thereto will be destroyed immediately or archived in anonymous form, following the principles further set out below. The Whistleblower will be informed of closure of the investigation.

When disciplinary or legal proceedings are brought against the person referred to in the report or against the Whistleblower, information relating to the report will be kept by the data controller until the end of those proceedings or the time limit for appealing against the decision.

In any event, the Group will comply with the following principles when dealing with retention of personal data processed in the context of the Mechanism:

- ✓ access to recorded / archived personal data will be restricted to authorized individual only;
- ✓ personal data will not be retained for a longer period than strictly necessary and proportionate in light of the processing purpose for which it is collected / processed (in accordance with Data Protection Laws).

Following the timeline of the investigations:

- ✓ personal data relating to an alert will be stored in an active databased until a final decision has been reached on the actions to be further taken;
- ✓ once the final decision on the actions to be taken on the alert has been reached, the relevant persona data may be kept in an intermediary archive database, for a period strictly proportionate to the processing of the reported information and to the protection of the Whistleblower, the involved persons and the third parties they mention, taking into account the time required for any further investigations;
- ✓ personal data may be retained for longer periods in an intermediary archive database if the Group is legally obliged to do so or for evidentiary purposes with a view to possible control or litigation, or for the purpose of carrying out quality audits of the Mechanism; and
- ✓ in any event personal data is archived in a confidential and secure way in accordance with applicable laws and regulations, including Data Protection Laws.

5. Observance of rights of information

The Group provides to individuals information required under Data Protection Laws at several stage of the treatment of an alert:

- ✓ The Group must inform all individuals potentially affected by the processing of alerts when the processing is deployed.
- ✓ The Whistleblower must also receive information about the treatment from the very start of the alert collection process.
- ✓ When the alert is issued, an acknowledgement of receipt must be provided to the

Whistleblower.

- ✓ The Group must also inform the person **who is the subject of an alert** (e.g., as a witness, victim or alleged perpetrator) within a reasonable period of time, and in any event, **up to one month** following the issuing of the alert, unless exceptions apply (. This information can be deferred notably if it is likely to seriously compromise the achievement of the processing purpose (e.g., if it would compromise the needs of the investigation). The information shall be delivered once the risk has been avoided.

Under the conditions and subject to the limitations provided by the regulations in force, the Group ensures that any persons identified in the context of the Mechanism will have the right to access information concerning them.

6. Data subjects' rights

Under the conditions and subject to the limitations provided by the regulations in force (including the Data Protection Laws), the Group ensures that any persons identified in the context of the Mechanism will have the right to exercise their rights of access to their data, right to have them corrected or deleted if it is incorrect, incomplete, ambiguous or out of date

More specifically, any person whose personal data is processed within the alert process has the right to query, access, complete, update, limit the processing of or delete personal information concerning them, notably when such personal data is incorrect, incomplete, ambiguous or out of date, or when the collection, use, communication or retention of which is prohibited.

For the avoidance of doubt, the right of rectification must not allow the retroactive modification of the information contained in the alert or collected during its investigation and the exercise of this right, when permitted, must not result in making it impossible to reconstruct the chronology of any changes to important elements of the investigation. Therefore, this right can only be exercised to rectify factual data, the material accuracy of which can be verified by the controller in support of evidence, without erasing or replacing the data, even erroneous, initially collected.

The right to erasure is exercised under the conditions provided for in Article 17 of the GDPR.

In addition, any person whose personal data is processed within the alert process can give instructions relating to the retention, deletion and communication of their personal information after their death, in accordance with the French LIL.

In order to exercise these rights, the relevant data subjects may notably send a request in writing, dated and signed, by registered letter to Plastic Omnium Gestion, 1 allée Pierre Burelle, 92593 Levallois Perret, marked for the attention of Group Data Protection Officer or by an-mail to dpo-group@plasticomnium.com stating their name, address and a telephone number at which they can be contacted during office hours.

Whistleblowers have also the right to request information regarding the decision taken following the submission of their alerts. When submitted anonymously, Whistleblowers can request information through a mean of contact allowing them to remain anonymous.

7. Technical and organizational security measures

The Group takes all precautions appropriate to the risks presented by its processing in the context of the Mechanism to protect the security of personal data and, in particular, at the time of collection, during their transmission and their retention, to prevent them from being distorted, damaged or accessed by unauthorized third parties. In particular, the Group will ensure that all appropriate measures are implemented by any processor intervening in the processing of the data within the Mechanism.

8. Record keeping of oral reports

Oral reports will be recorded according to the following processes:

- Where the report is made through a recorded telephone line or another recorded voice messaging system (with the consent of the reporting person), the report should be kept under a durable and retrievable format or accurately transcribed,
- Where the report is collected in the context of a videoconference or a physical meeting, it will be either formalized in a complete and comprehensive meeting minute, with the consent of the reporting person, or recorded, or accurately transcribed,
- When the report is made by telephone or any other unrecorded voice messaging system, the report must be completely and accurately transcribed.

In any case, the Group shall offer the possibility to the Whistleblower to review, amend and approve the transcript by signing it.

The recordings, transcripts and minutes may be kept only for as long as is strictly necessary and proportionate for the processing of the alert and for the protection of the Whistleblower, the persons to whom they refer and the third parties mentioned in them. The principles set out in Section 8 will also apply to the retention of such recordings, transcripts and minutes to the extent they contain personal data.

Local addendum

FRANCE

Subject matter	**Definition/rule**
Reporter	N/A
Whistleblower	Whistleblowers must act in good faith and without any direct financial compensation.
Protected third-party	N/A
Reportable concerns	N/A
Retaliation	N/A
Reports falling outside the protection	N/A
Confidentiality treatment	N/A
Anonymous reports	Acknowledgement and feedback requirements are not legally required for anonymous reports.
Acknowledge requirements	N/A
Feedback requirements	N/A
Impartiality	N/A
Record keeping and personal data	N/A
Special instructions with respect to record-keeping of oral reports	N/A
List of national competent authorities for external reporting	French authorities competent to receive reports include, without limitation:[1] • Agence Française Anticorruption (AFA) • Autorité des marchés financiers (AMF) • Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) • Autorité de la Concurrence • Commission nationale de l'informatique et des libertés (CNIL) • Défenseur des droits

[1] The full list of French authorities can be found in the decree No. 2022-1284 of 3 October 2022: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046357368.

Local addendum

BELGIUM

Subject matter	**Definition/rule**
Reporter	N/A
Whistleblower	N/A
Protected third-party	N/A
Reportable concerns	N/A
Retaliation	N/A
Reports falling outside the protection	With respect to "national security information", note that this indeed falls outside the protection but a carve-out should be added for reports of violations of public procurement rules in the fields of defence and security which should fall within the protection.
Confidentiality treatment	Any information that may reveal the identity of the whistleblower cannot be disclosed without his or her consent, ***except where a necessary and proportionate obligation exists under specific legislation in the context of investigations by national authorities or judicial proceedings***. In that case, the Whistleblower will be informed unless such information would jeopardize the ***related investigations by national authorities or*** judicial proceedings (instead of solely referring to "would not jeopardize the judicial proceedings" as set out in the whistleblowing procedure above).
Anonymous reports	Reports made by persons wishing to remain anonymous should ***always*** be dealt with by legal entities with more than 249 employees.
Acknowledge requirements	N/A
Feedback requirements	N/A
Impartiality	N/A
Record keeping and personal data	Not only the identity, functions and contact details of the Whistleblower can be recorded but also those of any person to whom the protection and support measures are extended. Personal data should be kept until the statute of limitation for the violation has lapsed. The Belgian legislator did not distinguish between the retention periods of those reports that effectively give rise to a follow-up and those that are declared inadmissible (as is the case in the whistleblowing procedure above).

	The Belgian law requires that the Belgian legal entity that sets up the Mechanism should be responsible for the processing of personal data. Therefore, the relevant Belgian entity should be mentioned in the whistleblowing procedure above instead of the French company Plastic Omnium Gestion, even if the processing is delegated internally. Complaints should accordingly be made to the Belgian Data Protection Authority (*Autorité de protection des données / Gegevensbeschermingsautoriteit*) instead of to the French Data Protection Commission (the "CNIL") and the relevant Belgian legal entity should also be handling requests for access, deletion and correction of personal information.
Special instructions with respect to record-keeping of oral reports	The recordings, transcripts and minutes are kept ***for as long as the contractual relationship with the whistleblower runs*** instead of "for as long as is strictly necessary and proportionate for the processing of the alert and for the protection of the reporting person, the persons to whom they refer and the third parties mentioned in them" as set out in the whistleblowing procedure above.
List of national competent authorities for external reporting	Belgian authorities competent to receive reports are the following, each in the context of their respective missions: • Service public fédéral Economie, PME, Classes Moyennes et Energie; • Service public fédéral Finances; • Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement; • Service public fédéral Mobilité et Transports; • Service public fédéral Emploi, Travail et Concertation sociale; • Service public de programmation Intégration Sociale, Lutte contre la Pauvreté, Economie Sociale et Politique des Grandes Villes; • Agence fédérale de Contrôle nucléaire; • Agence fédérale des médicaments et des produits de santé; • Agence fédérale pour la sécurité de la chaîne alimentaire; • Autorité belge de la Concurrence; • Autorité de protection des données; • Autorité des services et marchés financiers; • la Banque nationale de Belgique; • Collège de supervision des réviseurs d'entreprises;

	• Authorities referred to in Article 85 of the Act of September 18, 2017 on the prevention of money laundering and terrorist financing and on limiting the use of cash.Comité national de sécurité pour la fourniture et la distribution d'eau potable; • Institut belge des services postaux et des télécommunications; • Institut National d'Assurance Maladie-Invalidité; • Institut National d'Assurances Sociales pour Travailleurs Indépendants; • Office National de l'Emploi; • Office National de Sécurité Sociale; • Service d'Information et de Recherche Sociale; • Service autonome de Coordination Anti-Fraude (CAF); and • Contrôle de la Navigation. In the absence of designation of a competent authority for a specific subject matter or if no authority considers itself competent to receive a notification, the federal Ombudsmen (*les Médiateurs fédéraux* / *de Federale Ombudsmannen*) will act as the competent authority in Belgium.

Local addendum

Germany

Subject matter	**Definition/rule**
Reporter	N/A
Whistleblower	A whistleblower only enjoys protection under the German Whistleblowing Act (*Hinweisgeberschutzgesetz*, "**HinSchG**"), if the report is based on reasonable grounds and reasonable suspicion. Reporters are not required by law to submit any document or information likely to prove the facts alleged.
Protected third-party	N/A
Reportable concerns	In addition, the following concerns shall be reportable: • Violations regarding public procurement and concession procedures and pertaining to the legal protections in any such procedures above the relevant EU thresholds • Violations under Financial Services Supervisory Act • Violations of tax laws applicable to companies • Violations in the form of agreements aimed at obtaining a tax advantage in an abusive manner which is contrary to the objective or purpose of the tax law applicable to corporations and partnerships
Retaliation	N/A
Reports falling outside the protection	A whistleblower only enjoys protection under the Act (i.e., the non-retaliation principle) if the report is based on reasonable grounds and reasonable suspicion. On top of what is indicated in policy, the Act is not applicable to reports containing • Information from federal or state intelligence services, or from federal or state authorities or other public bodies, or • Information on public procurement and concession procedures under Article 346 of the Treaty on the Functioning of the European Union. Please refer to section 5 para 1 HinSchG for details. The Act does also not apply to reports conflicting with • Confidentiality and confidentiality obligations for the material or organizational protection of classified

	information • Obligation to safeguard lawyers'/notaries'/legal advisors'/patent attorneys', judges' or jury secrecy, and of any personnel assisting under contractual duty of confidentiality.
Confidentiality treatment	In summary, the identity of the Whistleblower may be disclosed • in criminal and administrative proceedings based the request of state prosecution or an order of the administrative body • on the basis of court decisions • in certain specific proceedings before the Federal Financial Supervisory Authority and the Federal Cartel Office, or • if the disclosure is necessary for follow-up measures and the Reporter has given consent.
Anonymous reports	Anonymous reports will be dealt with complying with all applicable rules, including the deadlines for communication with the Reporter.
Acknowledge requirements	N/A
Feedback requirements	N/A
Impartiality	N/A
Observance of rights of access and correction	Rights of access and correction are not bound to any formal requirements.

Record keeping and personal data	Documentation will, as a rule, be deleted three years after follow-up measures pursuant to section 18 HinSchG have been completed. Documentation can be stored for longer periods of time to meet the provisions of the HinSchG or other laws, as long as storage is necessary and proportionate.
Special instructions with respect to record-keeping of oral reports	According to section 11 para 2 HinSchG, if the report is made by telephone or any other voice messaging system, any recording or full transcription may only be produced with the consent of the Whistleblower (criminal sanctions). Otherwise, the discussion may merely be summarized.
List of national competent authorities for external reporting	German authorities competent to receive reports are: • Bundesanstalt für Finanzdienstleistungsaufsicht (reports concerning financial services, financial products or the financial markets, money laundering or the financing of terrorism) https://www.bafin.de/DE/DieBaFin/Hinweisgeberstelle/8_Zugang_zur_Hinweisgeberstelle/ZugangHinweisgeberstelle_node.html • Bundeskartellamt (reports concerning violations regarding competition law and for the law in force regulating digital markets) https://www.bundeskartellamt.de/DE/Kartellverbot/Anonyme _Hinweise/anonymehinweise_artikel.html • Bundesministerium der Justiz (reports concerning all other violations)

Local addendum

Austria

Subject matter	**Definition/rule**
Reporter	N/A
Whistleblower	N/A
Protected third-party	N/A
Reportable concerns	Breaches against Union and national acts in the areas set forth in Art 2 Par 1 of the Whistleblowing Directive. Additionally, violations of Sec 302 to 309 of the Austrian Criminal Code are reportable. Thus, not all crimes and offences fall in the scope of the HSchG.
Retaliation	N/A
Reports falling outside the protection	In addition to the areas listed in the group policy, reports in relation to the following areas are also excluded from the scope: (i) contractual agreements made to maintain confidentiality with partners or shareholders or supervisory bodies of notaries or business trustees, (ii) specific procurement procedures and (iii) chaplains.
Confidentiality treatment	The identity of whistleblower must not be disclosed within the company. Strict confidentiality obligations apply (even for reports to representatives). The identity of whistleblowers may only be disclosed if an administrative authority, a court or the public prosecutor's office deems this to be **absolutely necessary** within the framework of administrative or judicial proceedings or an investigation under the Code of Criminal Procedure and **proportionate** with regard to endangering the person of the whistleblower in view of the validity and seriousness of the allegations made (Sec 7 para 1, 3 and 5 and Sec 13 para 1 HSchG).
Anonymous reports	N/A
Acknowledge requirements	N/A
Feedback requirements	N/A
Impartiality	N/A
Record keeping and personal data	The HSchG provides for a retention period of five years from the last time the data was processed or transmitted and beyond that for as long as is necessary to carry out administrative or judicial proceedings that have already been

	initiated or investigative proceedings under the Code of Criminal Procedure (Sec 8 para 11 HSchG). Log Data must be stored for additional three years.
Special instructions with respect to record-keeping of oral reports	N/A
List of national competent authorities for external reporting	The Federal Bureau of Anti-Corruption and Corruption Prevention (*Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung*) is a general external body. For certain areas, there are exclusively competent external bodies: • Auditors' Supervisory Authority (*Abschlussprüferaufsichtsbehörde*) • the whistleblower system set up at the accounting authority (*Bilanzbuchhaltungsbehörde*) • the whistleblower system established at the Federal Competition Authority (*Bundeswettbewerbsbehörde*) • Financial Market Authority (*Finanzmarktaufsichtsbehörde*) • Money Laundering Reporting Office (*Geldwäschemeldestelle*) • the secure communication channels set up at the chambers of notaries (*Notariatskammer*) • the secure communication channels established at the bar associations (*Rechtsanwaltskammer*) • the whistleblower system set up at the Chamber of Tax Advisors and Auditors (*Kammer der Steuerberater und Wirtschaftsprüfer*) • Chamber of Tax Advisors and Public Accountants • Federal Disciplinary Authority as competent external authority of the Federal Ministry of the Interior including its subordinate offices

Local addendum

SPAIN

Subject matter	**Definition/rule**
Reporter	N/A
Whistleblower	N/A
Protected third-party	N/A
Reportable concerns	N/A
Retaliation	N/A
Reports falling outside the protection	On top of what is provided by the Policy, Information related to infringements in the processing of contracting procedures that contain classified information or that have been declared secret or reserved, or those whose execution must be accompanied by special security measures are also outside the protection.
Confidentiality treatment	N/A
Anonymous reports	The admission to processing will be communicated to the Whistleblowers within the following seven natural days, even if the communication was anonymous.
Acknowledge requirements	Acknowledgement of receipt must be sent to the Whistleblower no later than seven natural days after the alert's receipt (unless this might jeopardize the confidentiality of the communication). This also applies if the communication was anonymous.
Feedback requirements	N/A
Impartiality	N/A
Record keeping and personal data	In case the information provided is untrue, it shall be deleted immediately as soon as this becomes known, unless the untruthfulness could constitute a criminal offence, in which case the information shall be kept for the time necessary for the duration of the legal proceedings. In any case, if three months have elapsed since receipt of the communication and no investigation has been initiated, the information of the report shall be deleted.
Special instructions with respect to record-keeping of oral reports	N/A
List of national competent authorities for external reporting	Spanish authorities competent to receive reports include: • Independent Authority for the Protection of the Informant *(Autoridad Independiente de Protección*

	del Informante, AAI) At a regional level other authorities might be appointed (e.g., The Independent Whistleblower Protection Authority in Catalonia –the Anti-Fraud Office of Catalonia–, in accordance with Law 3/2023, of 16 March, on fiscal, financial, administrative and public sector measures for 2023). These regional bodies shall be competent in the regions in which the companies are domiciled, as a general rule.

Local addendum

ROMANIA

Subject matter	Definition/rule
Reporter	N/A
Whistleblower	N/A
Protected third-party	N/A
Reportable concerns	N/A
Retaliation	N/A
Reports falling outside the protection	N/A
Confidentiality treatment	N/A
Anonymous reports	Under Romanian law, anonymous reports are discarded if they are insufficiently detailed, but only if the investigator requested the remediation of the report and the anonymous reporter failed to do so within fifteen days.
Acknowledge requirements	N/A
Feedback requirements	N/A
Impartiality	N/A
Record keeping and personal data	Under Romanian law, records of reports must be retained for a period of five years, following which the records should be destroyed regardless of the storage medium.
Special instructions with respect to record-keeping of oral reports	Under Romanian law, transcripts of oral reports should also be retained for a period of five years. There is no express obligation to retain audio recordings.
List of national competent authorities for external reporting	Romanian authorities competent to receive reports include: • Public authorities and institutions which are tasked to receive and investigate reports in their areas of competence, such as: ○ *Consiliul Concurentei*, the Romanian competition authority, which established a whistleblowing portal for reports concerning anticompetitive behaviour [https://report.whistleb.com/ro/consiliulconcurente]; ○ *Directia Generala Antifrauda Fiscala*, the antifraud department of the Romanian tax authority which is

	entitled to receive tax or customs fraud reports via a special portal [https://www.anaf.ro/asistpublic/]; ○ *Directia Nationala Anticoruptie*, the Romanian anticorruption directorate [https://www.pna.ro/sesizare.xhtml]; ○ *Agentia Nationala de Integritate*, the National Integrity Agency (ANI) [https://avertizori.integritate.eu/]; ○ other public authorities and institutions to which the National Integrity Agency forwards reports for investigation.

Local addendum

POLAND

[

Subject matter	**Definition/rule**
Reporter	N/A
Whistleblower	N/A
Protected third-party	N/A
Reportable concerns	N/A
Retaliation	In addition to the list provided in the Policy, the definition of retaliation in the Polish draft act supplements the EU definition (article 5(11) of the Directive) by specifically mentioning the unwarranted initiation of oppressive proceedings against the Reporter as fulfilling the term.
Reports falling outside the protection	The Act will not apply to violations of law relating to public procurement in the fields of defence and security (apart from information's categorised in article 3(3) of the Directive).
Confidentiality treatment	N/A
Anonymous reports	At this stage, the legislator has not decided to introduce the possibility of implementing anonymous internal/external reporting as well as external reporting. As a rule, in order to effectively make a report, the reporting person will have to provide data identifying such person and enabling contact with such person. Anonymous reports will not be subject to the Act, which means that they may be left unprocessed. However, in the event that a legal entity or a public body decides to deal with anonymous reports, the relevant regulations on this issue will have to be included in the internal reporting procedure of the legal entity or the external reporting procedure of the public body, respectively.
Acknowledge requirements	N/A
Feedback requirements	N/A
Impartiality	N/A
Record keeping and personal data	In general, any data allowing to determine the identity of the Reporter shall not be disclosed, but for the express consent of the Reporter. The exceptions include cases where such disclosure is required by law, especially in public proceedings to guarantee the right of defense. The amount of personal data that can be stored and processed shall be limited only to that necessary for the receipt of the report or any subsequent

	action and shall be removed within 14 days of the determination that it is not relevant. All in all, personal data shall be removed upon the elapse of 4 years since the end of a calendar year when: the report was made, the subsequent actions were completed or the proceedings following the report were completed (whichever shall arrive last and unless they form part of court records).
Special instructions with respect to record-keeping of oral reports	N/A
List of national competent authorities for external reporting	An external notification is received by either the Polish Commissioner for Human Rights [link] or a public body (defined as " *the chief and central government administration bodies, field government administration bodies, state bodies with the exception of the Ombudsman, executive bodies of local government units, regional chambers of audit, the Chief of General Staff of the Polish Army and the Financial Supervision Commission*") which are to set out procedures. Each competent authority will display information concerning external reporting on its website, however since the law has not been adopted yet, such information may not be available.

Local addendum

CZECH REPUBLIC

Subject matter	**Definition/rule**
Reporter	N/A
Whistleblower	The whistleblower is not released from the general obligation to notify a public authority of the commission of certain criminal offences pursuant to Section 368 of the Act No. 40/2009 Coll., the Criminal Code, by using the internal whistleblowing system. These offences include for example murder, inhuman and cruel treatment, forgery and alteration of money, etc.
Protected third-party	N/A
Reportable concerns	N/A
Retaliation	N/A
Reports falling outside the protection	N/A
Confidentiality treatment	N/A
Anonymous reports	Anonymous whistleblowers are not protected from retaliation until their identity comes to light. In addition, the procedures set out in the Czech Whistleblowing Act do not apply to the handling of anonymous notifications (in particular as regards assessing their validity, the feedback requirements etc.) until the identity of the whistleblower is revealed.
Acknowledge requirements	The competent person shall notify the whistleblower in writing of the receipt of the notification within seven days from the date of receipt unless the whistleblower has expressly requested the competent person not to notify him, or notification of the receipt would disclose the identity of the whistleblower to another person.
Feedback requirements	The competent person must assess the validity of the notification and notify the whistleblower in writing of the outcome of the assessment within thirty days of receipt of the notification. In more complex cases, this time may be extended up to thirty days but not more than twice.
Impartiality	N/A
Record keeping and personal data	The notification and related documents must be kept for five years from the date of receipt of the notification.
Special instructions with respect to record-keeping of oral reports	The notification and related documents must be kept for five years from the date of receipt of the notification.

List of national competent authorities for external reporting	Ministry of Justice of the Czech Republic.

Local addendum

HUNGARY

Subject matter	**Definition/rule**
Reporter	N/A
Whistleblower	N/A
Protected third-party	N/A
Reportable concerns	N/A
Retaliation	N/A
Reports falling outside the protection	N/A
Confidentiality treatment	N/A
Anonymous reports	Acknowledgement and feedback requirements are not legally required for anonymous reports. In the case of anonymous Report, the employer has sole discretion to decide whether or not to investigate the Report.
Acknowledge requirements	The acknowledgement shall include general information to the Whistleblower on the procedural and data processing rules.
Feedback requirements	The operator of the internal whistleblowing system shall investigate the allegations contained in the Report within the shortest time possible under the circumstances, but not later than thirty days from the receipt of the Report. The thirty-day time limit may be extended in particularly justified cases, subject to simultaneous information of the whistleblower. In this case, the Whistleblower shall be informed of the expected date of the investigation and the reasons for the extension. The period for investigating the Report and informing the Whistleblower of the results of the investigation shall not exceed three months.
Impartiality	N/A
Record keeping and personal data	N/A
Special instructions with respect to record-keeping of oral reports	N/A
List of national competent authorities for external reporting	Hungarian authorities competent to receive reports include, without limitation (so called separate whistleblowing system): • the Directorate-General for Auditing European Aid, • the Hungarian Competition Authority,

	• the Integrity Authority, • the Public Procurement Authority, • the Hungarian Energy and Public Utilities Regulatory Office, • the Hungarian National Bank, • the National Authority for Data Protection and Freedom of Information, • the National Media and Infocommunications Authority, • the National Atomic Energy Authority; and • the Authority for the Supervision of Regulated Activities. In addition, the Government may, by decree, designate a body under the direction or supervision of the Government or a member of the Government to establish a separate whistleblowing system.

Local addendum

SLOVAKIA

Subject matter	Definition/rule
Reporter	N/A
Whistleblower	N/A
Protected third-party	N/A
Reportable concerns	N/A
Retaliation	N/A
Reports falling outside the protection	N/A
Confidentiality treatment	N/A
Anonymous reports	Acknowledgement and feedback requirements are not legally required for anonymous reports.
Acknowledge requirements	N/A
Feedback requirements	Feedback shall be provided within ninety days from the acknowledge of the report, or ninety-seven days from receiving the report.
Impartiality	N/A
Record keeping and personal data	Whistleblower can also make a complaint to Slovak Data Protection Authority. All reports (including oral reports and reports which are not considered substantial or justified) have to be archived for three years from the day of receiving them in the scope of: (i) receiving date, (ii) name, surname and residence of the Whistleblower provided that it is not an anonymous report, (iii) subject of the report, (iv) result of the investigation, and (v) finish date of the investigation. All such records are also required to be kept separately from any other records and/or registers.
Special instructions with respect to record-keeping of oral reports	Please see above "Record keeping and personal data".
List of national competent authorities for external reporting	Slovak authorities competent to receive reports: • Úrad na ochranu oznamovateľov[2] (*Office for the Protection of Whistleblowers*) • Prokurátor v rámci trestného konania (*Prosecutor's Office*)

[2] Available on https://www.oznamovatelia.sk/en/.

	• Orgán činný v trestnom konaní – prokurátor a policajt (*Law Enforcement Authorities – Prosecutor and Policeman)* • príslušný Správny orgán (*relevant Administrative Authority)*

TELEPNONE NUMBERS PER COUNTRY

Country	Hotline Number
Argentina	**0800-345-4304**
Austria	**0800-298-881**
Belgium	**0800-74-059**
Brazil	**0800-760-0085**
Canada	**833-269-5963**
China	**400-120-5039**
Czech Republic	**800-200-224**
France	**0-800-90-71-56**
Germany	**0800-181-5124**
Hungary	**06-80-019-670**
India	**022-5097-2720**
Indonesia	**(021)-5091-8364**
Italy (includes San Marino, Vatican City)	**800-836-928**
Japan	**0800-123-9455**
Malaysia	**1800-81-0780**
Mexico	**800-777-0153**
Morocco	**0530-525-244**
Poland	**800-005-346**
Romania	**0800-890-156**
Russia	**8-(800)-301-45-07**
Slovak Republic	**0800-002-300**
South Africa	**080-001-4673**
South Korea	**080-870-1687**
Spain	**900-751-361**
Switzerland	**0800-225-278**
Thailand	**1800-018-153**
Turkey	**00800-492-4088-0100**
United Kingdom & Northern Ireland	**0808-196-8132**
United States	**833-269-7638**