

Speak Up and Whistleblowing Policy

Additional Regional Supplement in relation to the European Union

This Additional Regional Supplement (“**Appendix**”) provides additional guidance in relation to the Group’s people and operations in the European Union (“**EU**”) (“**Cathay EU**”), in accordance with 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 (“**EU Whistleblowing Directive**”), and is subject to updates from time to time.

Any questions about specific points of national laws should be escalated to Group Compliance for consideration.

For the avoidance of doubt, this Appendix must be read together with the Group’s Speak Up and Whistleblowing Policy (“**Policy**”), and applies to whistleblowing reports made by any Whistleblower (defined below) in relation to Cathay EU. To the extent any part of the Policy or this Appendix sets out a higher standard or more stringent requirement, the higher standard or more stringent requirement shall apply.

1. Who is entitled to whistleblower protection

- 1.1 The following persons reporting on reportable matters (see Section 2.1 of this Appendix for further information regarding matters in respect of which a Whistleblower will be entitled to protection) in a “**work-related context**”¹ may be treated as a “**Whistleblower**” within the meaning of the Policy:
- (a) all Employees (including temporary agency workers, secondees, interns, volunteers, and paid or unpaid trainees) of any Group entity;
 - (b) any self-employed person dealing with any Group entity in a work-related context;
 - (c) any shareholder, director or person belonging to the administrative, management or supervisory body of any Group entity (including non-executive members); and
 - (d) any third party dealing with any Group entity in a work-related context (including contractors, subcontractors and suppliers), or any person working under its supervision and direction.²

¹ “**Work-related context**” means current or past work activities in the public or private sector through which, irrespective of the nature of those activities, a person acquires information on breaches and within which that person could suffer retaliation if he/she reported such information.

² A “**Whistleblower**” also includes any individual falling within Section 1.1 of this Appendix where:

- (a) he/she has ceased to be a Whistleblower as set out above, provided that the information on reportable matters was acquired during his/her relationship with the Group; or
- (b) his/her relationship with the Group is yet to begin, provided that the information on reportable matters has been acquired during a recruitment process or other pre-contractual negotiations.

1.2 A “**Whistleblower**” will qualify for protection if he/she:

- (a) makes a report internally³ or externally⁴ on “**information on breaches**”⁵ (see Section 2.1.1 of this Appendix for further information regarding “**breaches**” that are within the scope of the Policy); and
- (b) has reasonable grounds to believe that the information reported was true at the time of reporting.

The protection is also available to any person who assists the Whistleblower in the reporting process in a work-related context (also known as “**facilitator**”), and third parties and legal entities connected to the Whistleblower (see Section 3.1 of this Appendix).

2. Reportable Matters

2.1 Matters in respect of which a Whistleblower will be entitled to protection (provided that the conditions in Section 1.2 above are met) include the following:

2.1.1 “**Breaches**”, which refer to acts or omissions that are unlawful under (or contrary to the object or purpose of) relevant EU legislation (and national laws, as applicable) in the following areas, irrespective of whether they are reported by way of internal reporting, external reporting or public disclosure⁶:

- (a) public procurement;
- (b) financial services, products and markets, and prevention of money laundering and terrorist financing;
- (c) product safety and compliance;
- (d) transport safety;
- (e) public health;
- (f) consumer protection;
- (g) protection of privacy and personal data, and security of network and information systems;
- (h) breaches relating to the internal market, including EU competition law and state aid rules, and acts that breach the rules of corporate tax or arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;
- (i) breaches affecting the financial interests of the EU, such as fraudulent activities;
- (j) breaches that would constitute serious infringements of criminal or administrative law under national laws of any EU member state (including bribery and corruption and, in the whistleblowing context,

³ “**Internal reporting**” means the oral or written communication of information on Breaches within the Group.

⁴ “**External reporting**” means the oral or written communication of information on Breaches to competent authorities in the EU and/or individual EU member states.

⁵ “**Information on breaches**” means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in a Group company in which the Whistleblower works or has worked, or in another organisation with which the Whistleblower is or was in contact through his / her work, and about attempts to conceal such breaches.

⁶ “**Public disclosure**” means the making of information on Breaches available in the public domain.

hindering or attempting to hinder reporting, and retaliation against a Whistleblower);

- (k) other areas such as protection of the environment, radiation protection and nuclear safety, food and feed safety, animal health and welfare; and
- (l) any other areas in respect of which the Whistleblower may be protected under applicable national laws.

Any attempt to conceal any such Breaches would also constitute a Breach.

2.2 Reports that are out of scope. Reports that fall within the following categories are generally not protected (and should not be reported via the reporting channels under the Policy):

- (a) reports relating to personal work-related grievances or disputes, such as complaints about interpersonal conflicts, or that affects only the Whistleblower and the individual(s) subject to the report;
- (b) reports relating to matters that are already fully available in the public domain, or constitute mere rumours; and
- (c) reports that do not relate to matters covered in Section 2.1.1 of this Appendix.

3. What protections are available

3.1 Protection against retaliation

The Group prohibits any retaliation (or any threat or attempt to retaliate) against:

- (a) a Whistleblower;
- (b) a facilitator;⁷
- (c) any third person connected with the Whistleblower and who could suffer retaliation in a work-related context (such as a colleague or relative / family member of the Whistleblower who at the same time has a work-related connection with the Group); and
- (d) a legal entity which the Whistleblower owns,⁸ works for or is otherwise connected with in a work-related context,

provided that the Whistleblower had reasonable grounds to believe that the information on which he/she makes the report was true at the time of reporting. The protections provided in the Policy will not be extended to anyone who knowingly makes a false report.

Retaliation means any direct or indirect act or omission which occurs in a work-related context, prompted by the Whistleblower's report, and which causes or may cause unjustified detriment to the Whistleblower and/or any of the persons or entities eligible for protection in (b) – (d) above.

⁷ In Spain, this expressly includes legal representatives of workers in the exercise of their functions of advising and supporting the Whistleblower.

⁸ Under Spanish Law 2/2023, this applies where the Whistleblower has a significant shareholding of a legal entity. A shareholding is "significant" where it accords the person the ability to influence the legal entity.

Examples of retaliation include:

- (a) suspension, layoff, dismissal or equivalent measures;
- (b) demotion or withholding of promotion;
- (c) a negative performance assessment or employment reference;
- (d) transfer of duties, change of location, reduction in wages, or change in working hours;
- (e) withholding of training;
- (f) imposition or administering of any disciplinary measure, reprimand or other penalty (including a financial penalty);
- (g) failure to convert a temporary employment contract into a permanent one, where the person had legitimate expectations that they would be offered permanent employment, or failure to renew, or early termination of, a temporary employment contract;
- (h) coercion, intimidation, harassment or ostracism;
- (i) discrimination, disadvantageous or unfair treatment;
- (j) harm to a person's financial position (such as loss of business or income) or reputation (such as in social media);
- (k) blacklisting, whether formally or informally agreed, which may hinder or prevent a person's access to employment or the contracting of works or services in the relevant sector or industry;
- (l) early termination or cancellation of a contract for goods or services;
- (m) denial or cancellation of a licence or permit; or
- (n) psychiatric or medical referrals.

If any Whistleblower believes that they have been subject to retaliation as a result of a report being made, they should report it immediately through the Company's internal channels in accordance with the Policy. Any Employee who is found to have engaged in retaliation or causing a detriment to any person as a result of a report being made will be subject to disciplinary action, including potential termination of employment.

3.2 Identity protection

Subject to exceptions, the Group will take reasonable steps to protect the confidentiality of the identities of the Whistleblower, any person mentioned in a report, and/or any person who assists the Whistleblower in the reporting process, including any other information from which their identities may be directly or indirectly deduced.

In this regard, we will ensure the following:

- (a) **All Employees and other individuals authorised to have access to reports made under the Policy are aware of their confidentiality obligations; and that any breach of such obligations would be a serious infraction.**

- (b) **We will not disclose the identity of the Whistleblower (or any other information from which his/her identity may be directly or indirectly deduced) to anyone other than authorised members of the Group responsible for receiving or following up on reports, without the Whistleblower's explicit consent.**

However, there may be circumstances where we are required under EU or national laws to make a disclosure of the above information, including to judicial or national authorities in the context of judicial proceedings or investigations conducted by national authorities. Where we are required to make such disclosure, we will inform the Whistleblower of the same (unless such information would jeopardise any related investigations or proceedings).

4. How to report a concern under the Whistleblowing Policy

4.1 Internal reporting

Please refer to Section 6.1 of the Policy for the various channels through which a Whistleblower may report concerns internally under the Policy.

In addition to the channels set out under Section 6.1 of the Policy, if requested by the Whistleblower, a physical meeting will be arranged by Group Compliance within a reasonable timeframe in accordance with any requirements under applicable national laws.⁹

The above reporting channels are managed by members of Group Compliance, which is an impartial and qualified team authorised and appointed by the Group to receive, assess and take action on all reports received under this Policy.

4.2 External reporting and public disclosure

While the Group encourages Whistleblowers to report internally, Whistleblowers may make a report on any Breach directly to competent EU or national authorities, which will afford them protection under the relevant whistleblower protection laws.¹⁰

A Whistleblower who makes a public disclosure relating to any Breach will only be eligible for protection under the Policy if the conditions set out in Section 1.2 of this Appendix and one of the following conditions are met:

- (a) a report has been made through internal or external reporting channels (or both) under this Policy, but no appropriate actions (such as the acknowledgement of receipt of the report, provision of feedback and conclusion of the investigation) have been taken within a reasonable timeframe;¹¹

⁹ In Spain, where a Whistleblower requests for a face-to-face meeting to make a report, a meeting will be arranged and take place within seven calendar days.

¹⁰ In Spain, external whistleblower reports may be made to the **Independent Authority for the Protection of Informants** (*Autoridad Independiente de Protección del Informante*) ("**AAI**"). As at the date of this Appendix, the national AAI has not been established yet.

Pending creation of the national AAI, a Whistleblower may make a report to regional competent authorities such as:

(i) in Catalonia (*Catalunya*), the Catalan Anti-Fraud Office (*Oficina Antifrau de Catalunya*) via [Report corruption | Oficina Antifraude de Catalunya](#); and

(ii) in Valencia (*València*), the Valencian Anti-Fraud Agency (*Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana*) via [Complaint Mailbox - Antifraucv](#).

¹¹ What is "reasonable" would depend on the timeframes for each relevant action, as set out in Section 5 of this Appendix.

- (b) the Whistleblower has reasonable grounds to believe that:
 - (i) the Breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or
 - (ii) in the case of external reporting, there is a risk of retaliation or there is a low prospect of the Breach being effectively addressed due to the particular circumstances of the case.¹²

5. Investigation procedures and outcome

5.1 For details of the key steps that may follow the receipt of a report, please refer to Section C of the Policy. However, the actual process may vary depending on the nature of the report. Please also note the following:

- 5.1.1 **Acknowledgement of receipt.** Reports received will be acknowledged within 7 calendar days (or any shorter period as required by national laws), unless such acknowledgment would jeopardise the protection of the confidentiality of the report.
- 5.1.2 **Investigation timeframe.** Where we determine that an investigation is required, we will commence an investigation as soon as reasonably practicable, and aim to conclude any investigation within a reasonable timeframe subject to any requirements under applicable national laws from the date of our receipt of any report. However, the actual timeframe may vary depending on the complexity of the investigation.¹³
- 5.1.3 **Investigation progress updates and conclusion.** Where contactable, the Whistleblower will be provided with updates on the investigation process (including steps planned or taken in response to the report, and the underlying reasons) as appropriate within a reasonable timeframe, and in any case, no later than 3 months from the acknowledgment of receipt (or within such timeframe as prescribed by national laws), and its conclusion as appropriate. The availability and frequency of these updates may vary depending on the nature of the matter and complexity of the investigation. Where possible, we will maintain communications with the Whistleblower, including to request for additional information in relation to the report.
 - (a) To maintain communication with us (including to receive our progress updates and provide additional information if needed), the Whistleblower is encouraged to provide an email address (or postal address), or indicate a safe channel through which he/she can be contacted.
 - (b) In some cases there may be certain limitations to the level of information regarding an investigation that can be provided to a Whistleblower, and there may be circumstances where it may not be appropriate to provide details of the outcome of an investigation to the Whistleblower (e.g. due to privacy concerns).

¹² For example, where evidence may be concealed or destroyed, or where an authority may be in collusion with the perpetrator of the Breach or involved in the Breach.

¹³ In the case of reports made in or from Spain, we will complete an investigation by no later than 3 months (and for complex cases, no later than 6 months) from the date we acknowledge receipt of a report.

- 5.1.4 **External reporting.** In the context of each report, we will consider the Group's obligation to make any follow-on reports to competent authorities.¹⁴
- 5.1.5 **Fair and due process.** We are committed to ensuring fair and consistent treatment of all individuals who are involved in an investigation, including those who are under investigation or those whose identities become relevant in the course of an investigation. Without prejudice to the confidentiality protection offered to the Whistleblower under the Policy and to the extent permitted by law, persons subject to an investigation will be offered the opportunity to respond to any allegations made against them. The presumption of innocence and the honour of such persons concerned will be respected.
- 5.1.6 **Record-keeping.** Any processing of personal data (including the Whistleblower's personal information) contained in a report made under the Policy or obtained as part of any investigation relating to such report will be carried out in accordance with Regulation (EU) 2016/679 (GDPR) and any applicable national laws.

Effective date – 14 October 2025

¹⁴ For example, in Spain, if the facts of a report made under the Policy indicate the potential commission of a criminal offence, we are legally obliged to forward such information to the Public Prosecutor's Office. If the facts could affect the financial interests of the EU, we are similarly obliged to refer the case to the European Public Prosecutor's Office.