



Worldwide Flight Services Whistleblowing Policy

Edition 2 – June 2023



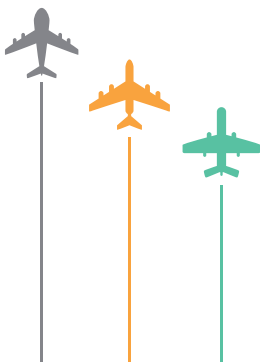
A Member of the SATS Group

WFS («WFS» or the “Company”) is fully committed to achieving the highest standards of honesty, integrity and ethics. It is the responsibility of every employee of WFS to ensure that no inappropriate behaviour takes place that could compromise the interest of our employees, shareholders, investors, third parties and the wider public. To that end, WFS has implemented this Policy as a reflection of our commitment to conducting our business in an ethical, compliant and responsible manner.

This Policy outlines how WFS will assist individuals in expressing their concerns securely, identifying whom to approach, and the reporting process while ensuring their protection, accounting for data protection requirements and legal provisions.

There may be instances where this Policy is at variance with the local laws of a particular country. Where local law imposes higher standards than those set out in this Policy, the local law will apply. If by contrast, the Policy provides for a higher standard, it will prevail, unless such compliance would be in violation of local law.

Good knowledge and understanding of this Policy are essential to its effectiveness. Therefore, it has been widely disseminated using various means, including digital communication or face-to-face presentations, poster campaigns, etc.



1. The Scope of the Policy

1.1. Who can report an Alert under the Policy?

Individuals falling within the categories listed below, whether currently or formerly associated with the Company, have the authority to report Alerts:

- Shareholders;
- Members of the administrative, management, or supervisory body, which may include non-executive members;
- Employees, trainees, interns, people who participate in selection processes or volunteers;
- Contractors, including customers and suppliers, and their employees;
- Associates of WFS or related entities; or,
- Spouses, relatives or any other person providing assistance to the reporting person of any of the categories listed above.

To ensure compliance with this Policy, individuals falling within the aforementioned categories are encouraged to report any irregularities or non-compliance they become aware of, without fear of dismissal or retaliation, and with the assurance that any information provided will be treated with the utmost confidentiality.

The term 'Whistleblower', as used in this Policy, refers to an individual who falls within the aforementioned categories and who reports any concerns under the scope of this Policy.

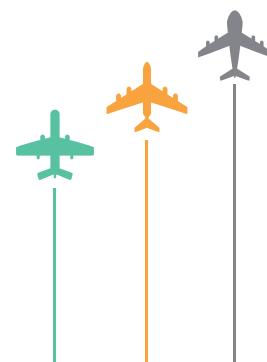
1.2. Who can be reported?

Individuals who are affiliated with WFS and act on behalf of or for the benefit of WFS are subject to reporting if they engage in any irregularities or behaviors that fall within the scope of this Policy. This includes, but is not limited to, directors, managers, employees, contractors, suppliers, and any other person or entity associated with WFS.

1.3. Which concerns may be reported?

An Alert may be reported only to raise in good faith any known or reasonably suspected concerns related to those behaviours that violate the internal policies of the Company, applicable laws or regulations or the general interest, especially those that:

- are classified as criminal offences or misdemeanours under the local laws and regulations;
- entail fraud or misconduct relating to accounting and auditing;
- involve fraud or misconduct relating financial and banking matters;
- comprise serious and apparent violation of the law and/or regulations or an international commitment ratified or approved by the relevant country;
- constitute an administrative infringement;
- imply a threat or serious prejudice to the public interest;



- may attribute responsibility or any kind of harm or discredit to WFS;
- constitute any information, knowledge, experience or any other circumstance that the Whistleblower considers relevant to bring to the attention of WFS, due to its direct relation to ethical issues of the internal management or to the compliance regulations of WFS.

Likewise, the material scope of the Policy includes any ethical inquiry to WFS regarding the values, principles, norms, or criteria contained in its Code of Conduct or any other internal regulations.

Examples of matters include:

theft, money laundering, embezzlement, and fraud;

misconduct relating to accounting and auditing;

bribery and corruption;

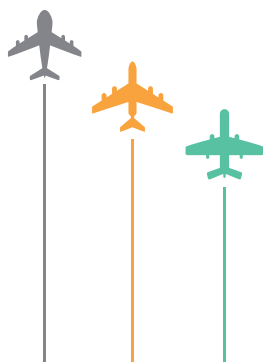
- antitrust and competition law issue;
- export controls, economic sanctions and embargoes;
- discrimination or harassment at work;
- health, hygiene and safety at work;
- environment protection;
- breach of WFS' policies and procedures.

This list is not exhaustive, and these areas are likely to evolve over time.

A Whistleblower may not use the reporting channels outlined in this Policy to report general complaints or personnel-related matters, such as interpersonal conflicts between employees, conflicts between employees and their managers, issues related to employment contracts, performance related issues, termination, disciplinary matters, and other similar issues. Such types of matters should be addressed to the line manager, the Legal Department or any member of the Human Resources Department.

1.4. Person responsible for the Policy

The management of the Policy will be the responsibility of the Risk and Compliance Committee led by the Compliance Officer for the purposes of this Policy.



2. General Principles

2.1. Protection of the Whistleblower's Identity

WFS wants to ensure that reporting an Alert through the available channels is a secure place for everyone involved, especially for the Whistleblower, but also for all its employees, and affiliates, irrespective of their position within the Company. This involves maintaining strict confidentiality. To achieve this, it is explicitly stated that the accused party's (the "Reported Party") right to access information under GDPR does not extend to information regarding the Whistleblower's identity. Individuals who possess knowledge of the reports made through these channels for investigative and decision-making purposes are obligated to maintain confidentiality regarding the Whistleblower's data, particularly their identity. However, if the Whistleblower deliberately releases their identity in a public disclosure, the confidentiality of the Whistleblower or third parties cannot be guaranteed.

2.2. Protection of the Whistleblower

To ensure the protection of individuals who report irregularities or behaviors in good faith, it is crucial that the Whistleblower believes, based on the available circumstances and information at the time of disclosure, that the facts they report are accurate and true. This is a necessary precaution to guard against false and malicious reports and ensures that those who intentionally provide incorrect or misleading information are not protected. However, unintentional inaccuracies in the disclosure will not negate the Whistleblower's protection. The Whistleblower's reasons for the disclosure are irrelevant to the proper functioning of the reporting channels. Protection is also extended to individuals who raise reasonable doubts or suspicions about reported facts, even if they do not have conclusive evidence. Whistleblower protection includes protection against retaliation taken against the legal entity for which the Whistleblower is an owner, employee, or otherwise associated in a work context. This includes measures such as the denial of services or any other similar practices.

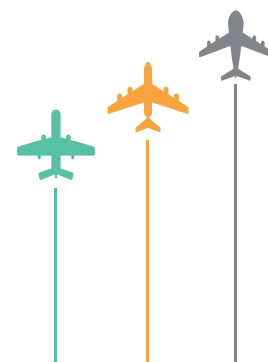
2.3. Prohibition of Retaliation

To guarantee legal protection, it is imperative to prevent any form of retaliation against individuals who report alleged misconduct in good faith under the scope of this Policy. Retaliation refers to any negative consequences that a Whistleblower may suffer as a direct or indirect result of their disclosure.

For this reason, WFS will safeguard the Whistleblower against any form of retaliation, discrimination, or punishment arising from reports made in good faith. However, it should be noted that if an internal investigation determines that a Whistleblower intentionally provided false or misleading information, appropriate disciplinary action may be taken.

2.4. Protection of Third Parties in the procedure

Any procedures related to this Policy will enable the protection of the identity of all parties involved in the report, throughout all stages of the whistleblowing procedure, subject to the legal conditions and requirements set up for external or public reporting.



2.5. Whistleblower Counseling

The Compliance Officer will provide individualized advice and accurate information to the Whistleblower concerning the responsible exercise of their reporting faculty.

2.6. Legal or contractual obligations as a reason for dismissing reports

Legal or contractual obligations of individuals, such as loyalty clauses, professional secrecy or non-disclosure agreements, cannot be invoked to prevent reports, deny protection, or penalize the Whistleblowers who provide information that falls within the scope of such agreements. When these conditions are met, the Whistleblower cannot be held liable for any civil, criminal, administrative or labour-related actions. However, the Whistleblower may be held accountable if they provide false or misleading information without sufficient grounds.

2.7. Whistleblower's Immunity

A Whistleblower who reports misconduct using legally obtained information or documents cannot be held accountable for any legal action that may arise from their report, regardless of whether they shared the information or made copies. This protection extends even if the Whistleblower's actions violate their employment contract. However, if the information or documents were obtained illegally, such as through physical or computer intrusion, the Whistleblower may be held criminally liable under applicable laws. It is important to note that the Whistleblower is responsible for any actions or omissions that are not related to the report or are not necessary for the disclosure of the violation.

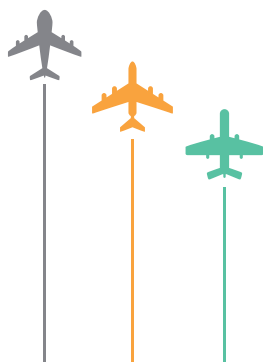
It should be noted that the immunity provided to the Whistleblower does not apply to facts, information or documents (regardless of their form or medium) covered by the national defence secrecy, medical secrecy or legal privilege.

2.8. Privacy Protection in the Whistleblowing Policy

The personal data collected as part of any communication or report is subject to protection under the applicable legislation regarding the protection of personal data. To learn more about this, please refer to **Appendix 4 "Privacy Statement"**, which is included in this Policy.

2.9. Existence and Management of Conflict of Interest

WFS's Compliance Officer is responsible for managing conflicts of interest to ensure that individuals connected to a communication or report do not participate or have any influence in the proceedings or investigation, in order to prevent any potential bias or unfairness.



3. Channels to report an Alert

A variety of reporting channels are available to report an Alert, allowing a Whistleblower to choose the most suitable channel taking into account the particular circumstances of the matter.

3.1. Group Reporting System (“Ethics Hotline”)

In order to ensure a secure and efficient reporting process, WFS has engaged a third-party service provider, CONVERCENT, to host and administer the Ethics Hotline. Upon receipt of a report, the appointed personnel with a legitimate right to access it based on their assigned responsibilities under this Policy, will promptly review it, while ensuring strict access control for personal data and confidentiality.

A Whistleblower has access to the reporting system, 24/7 through the following channels:

- Online tool: any Whistleblower can file a report using the online tool available at <http://app.convercent.com/>.
- Call Center: a Whistleblower can also contact the call center at the telephone numbers listed in the Appendix 1 of this Policy.

3.2. Mail – e-mail

An Alert can also be submitted via postal mail. It is recommended to send the letter via registered mail with acknowledgement of receipt to the following addresses:

Mail:

WFS Global
Compliance Officer - Whistleblowing Policy
7 boulevard de la Madeleine
75001 Paris

E-mail:

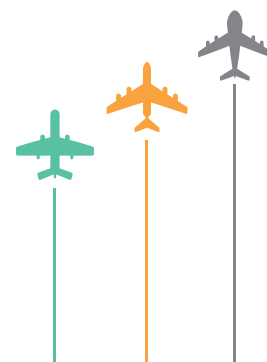
whistleblowing@wfs.aero

3.3. Compliance Champions

If the Whistleblower prefers, concerns can also be raised with the Compliance Champion in their country through in-person meetings, emails or mailed correspondence. The contact information of the Compliance Champions can be found in **Appendix 2** of this Policy.

3.4. External or public reporting channels

A Whistleblower has the possibility to use external or public reporting channels in compliance with the legal conditions and requirements set up for these.



3.5. Miscellaneous

If individuals choose to make a report through email, regular mail or verbally it is preferable that they use the Reporting Form provided in **Appendix 3** of this Policy.

Please note that any report submitted through channels other than those specified above may not be accepted and could be disregarded.

While most of the available reporting channels allow a Whistleblower to report Alerts anonymously, WFS encourages any Whistleblower to identify while submitting the report/s in a strictly confidential manner. Non-anonymous reports are normally handled in a more efficient way. If a Whistleblower chooses to remain anonymous, WFS encourages the use of the Ethics Hotline to report an Alert. Anonymous Alerts are handled with increased caution, and their admissibility will depend on the seriousness of the facts and the level of detail provided regarding the evidence and supporting factual elements.

The Whistleblowers are encouraged to describe their concerns as objectively and thoroughly as possible.

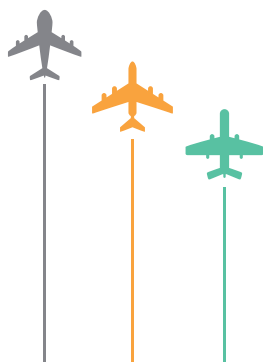
4. Processing of the Alerts

4.1. Receipt of communications and/or reports

Any Alert received shall be sent, without undue delay, to the Compliance Officer who is exclusively responsible for evaluation of all communications and/or reports submitted through the relevant channels. When deemed necessary, the Compliance Officer will receive support from the Human Resources or any other concerned Department, or from the local Compliance Champion in the country where the concern was raised.

4.2. Notification of actions to the Whistleblower

The Whistleblower will be notified of the receipt of their Alert within seven (7) business days from the date of submission (i.e. determining whether it falls within the scope of this Policy). The Whistleblower will be kept informed of the progress and outcome of the investigation. As part of a preliminary analysis of the Alert, the Whistleblower may be asked to provide additional information. If an Alert is received that falls outside the scope of this Policy, it will be promptly deleted.



4.3. Corrections of the content of communications and/or concerns raised

In the event that deficiencies in the communication and/or report are detected, the Whistleblower will be promptly notified of such deficiencies. If the requirements are not corrected within (5) five business days from the day following the notification, the report will be rejected, and subsequently archived, and no investigation will be initiated.

The Compliance Officer will acknowledge receipt of the Alert, the decision taken, its archive when applicable, and the grounds for such decision. This decision by the Compliance Officer shall not prevent the subsequent initiation of an investigation if additional information is received.

If the report is rejected, the Compliance Officer shall inform the Whistleblower in writing at the contact address provided, specifying and justifying the reason(s) for the rejection. If new information of a similar nature to that already considered is received, this resolution by the Compliance Officer will not hinder the launch of a subsequent investigation. The Whistleblower may be asked to provide additional information during the investigation, but it is not a mandatory requirement. Additionally, the Whistleblower will be notified of the progress of the investigation and any other anticipated responses during the evaluation of the appropriate processing for the communicated report.

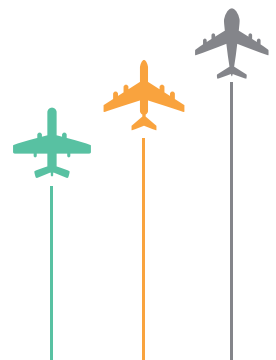
The processing and response to the Whistleblower shall occur within a reasonable period not exceeding (3) three months. However, in specific circumstances, depending on the nature and complexity of the matter, the investigation may require up to (6) six months. The Whistleblower will be notified upon completion of the investigation, and the file shall be closed. The Whistleblower may provide any information he/she deems appropriate in order to reopen the file.

4.4. Court review of the reported facts

The Whistleblower will have the right to do a Court review of the communicated report.

4.5. Rejection of Communication and/or Concerns

If the Alert does not fulfill the necessary formal requirements or the reported facts do not constitute a violation within the objective scope of the Policy, the Whistleblower will be informed of its rejection.



Grounds for rejection may include, but are not limited to:

- a) Communications and/or Alerts received via non-designated channels;
- b) Non-compliance with formal requirements;
- c) Facts that fall outside the Policy's objective scope;
- d) Vague or imprecise descriptions of reported facts;
- e) Facts that have nothing to do with the Company or Alerts that repeat previously reported incidents.

4.6. Communication of Actions to the Reported Party

Upon receiving an Alert or public disclosure that names a person as the Reported Party in an infringement, the Reported Party will be informed, within the time and manner deemed appropriate to ensure the conduct of the investigation, of (i) the receipt of the Alert, (ii) the specific allegation(s) made against the Reported Party, and (iii) the departments and third parties who may receive the Alert. In addition, (iv) the Reported Party will be provided with guidance on how to exercise their data protection rights in accordance with relevant regulations.

However, if the Compliance Officer deems that notifying the Reported Party would compromise the investigation, destroy evidence or proof, or disrupt the Company's normal operations, such communication may be postponed until such risks are eliminated.

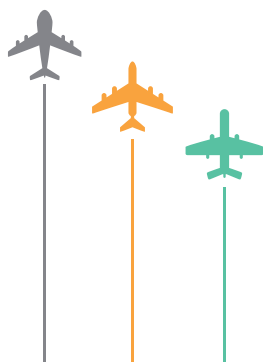
In any event, WFS will comply with the deadlines established by law for informing the Reported Party from the receipt of the Alert.

5. The Reporting Obligation of the Compliance Officer

The Compliance Officer shall periodically, and at least once a year, report to the Company's Management on the implementation of this Policy and its effective compliance.

6. Update and Review of the Policy

This Policy will undergo regular reviews and updates as necessary, to ensure compliance with relevant laws and promote the sharing of best practices, in order to ensure that the established procedures remain appropriate for functioning of the channels and their intended purpose.



List of Appendices

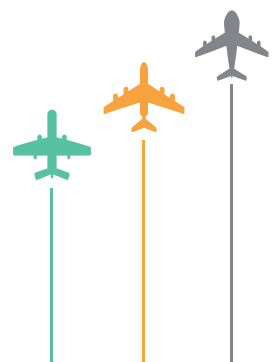
Appendix 1: Group Reporting System Call Center telephone numbers

Appendix 2: WFS Compliance Champions

Appendix 3: Reporting Form

Appendix 4: Privacy Statement

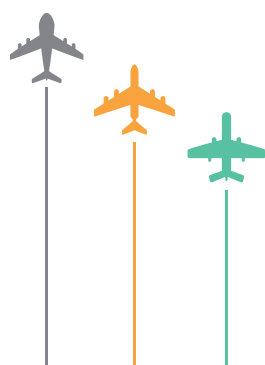
Appendix 5: Definitions



Appendix 1: Group Reporting System Call Center telephone numbers

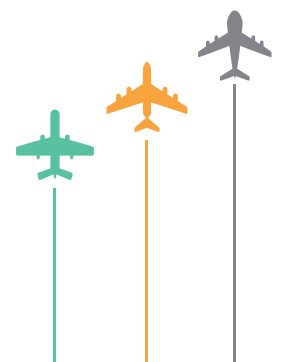
Country	Number
Albania (Tirana)	4 454 1957
Algeria	982402369
Andorra	00 800 1777 9999
Angola (Luanda)	226434276
Antigua	1-855-385-4107
Argentina	0800-333-0095
Australia	1 800 763 983
Austria	800 281119
Bahamas	1-855-271-0889
Bahrain	800 06 488
Bangladesh	(0) 9610 998400
Barbados	1-855-203-6928
Belarus	8 820 0011 0404
Belgium	0800 260 39
Belize	1 800 017 6274
Benin (Parakou)	61012482
Bermuda	1-855-579-9534
Bolivia	800 104 008
Bosnia & Herzegovina	080-083-038

Country	Number
Botswana	00269 800 3002 116
Brazil	0 800 892 2299
Brazil (Rio de Janeiro)	21 2018-1111
Brunei	801 4144
Bulgaria	0800 46038
Burkina Faso	25300026
Cambodia (Phnom Penh)	23962515
Canada	1-800-235-6302
Cayman Islands	1-855-475-9296
Chile	800-914-012
China	400 120 3062
Colombia	01-800-5189703
Colombia (Bogota)	6013816523
Costa Rica	4000-3876
Croatia	0800 806 520
Curacao	9 7889979
Cyprus	8009 4544
Czech Republic	800 701 383
Denmark	8082 0058



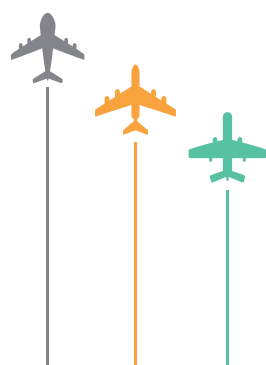
Dominican Republic	1-829-200-1123
Ecuador	1 800 000 138
Egypt	0800 000 0413
El Salvador (San Salvador)	2113-3417
Estonia	800 0100 431
Ethiopia	800-86-1917
Finland	0800 07 635
France	0805 080339
Georgia	706 777493
Germany	0800 181 2396
Ghana	24 2426201
Greece	00800 1809 202 5606
Greece (Athens)	21-1198-2708
Grenada	1-855-304-7847

Honduras	800-2791-9500
Hong Kong	800 906 069
Hungary	212111440
Iceland	800-4256
India	000 800 100 3428
India	000 800 100 4175
India (Kolkata)	337-1279005
Indonesia	0800 1503216
Ireland	1800 904 177
Israel	1 809 477254
Israel (Jerusalem)	2-375-2169
Italy	800 727 406
Ivory Coast	0566770939 1 855 271 0889
Jamaica	1-876-633-1693



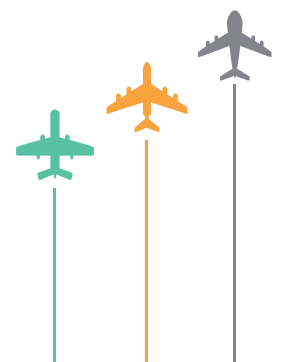
Guam	833 444 0484
Guatemala (Guatemala City)	2378-4832
Jordan	0800 22656
Kazakhstan	8 800 333 3511
Kenya	0800 221312
Kenya (Nairobi)	20 3892291
Korea, Republic of (South Korea)	080 880 0476
Kosovo – Pristina	38-403-005
Kuwait	227-9501
Kyrgyzstan	00 800 13337 289
Laos (via Singapore)	+65 3158-9628
Latvia	8000 4721
Lebanon *Number is 2-step	01 426 801 then 855- 8659-450
Lithuania	8 800 30451
Luxembourg	800-27-311
Macau	6825-8516
Macedonia	0800 93894
Malawi	800 026 9819
Nigeria	070 80601844

Japan	0800-170-5621
Japan	001 800 1777 9999
Malaysia	1548770383
Mali	449 60005
Malta	8006 2783
Mauritius	802 049 0005
Mexico	800 681 6945
Moldova	0800 69006
Monaco	80094461
Montenegro (Podgorica)	38220405847
Morocco (Casablanca)	5204 85014
Mozambique	29 000 000
Myanmar (Yangon)	1 239 0053 0800 800 8023
Namibia (Windhoek)	833300079
Nepal	1 800 001 0106
Netherlands	0-800-022-0441
New Zealand	0800-002-341
Nicaragua (Managua)	2248-2265 001 800 220 1152
Democratic Republic of Congo	064000036



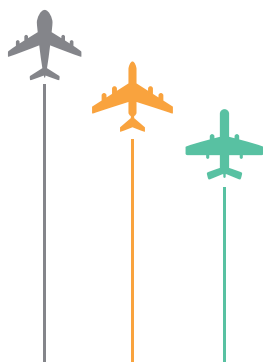
Nigeria	1 227 8917
Norway	800 62 492
Oman	800 74295
Pakistan (Islamabad)	51 8108900
Panama	800 2066
Papua New Guinea	000861204
Paraguay	009 800 542 0162
Paraguay	+595 21 728 9731
Peru	0800 78323
Philippines (Manila)	2 86263049
Poland	00-800-111-3819
Poland	00-800-141-0213
Portugal	800 180 367

Romania	0-800-360-228
Russia	8-800-100-9615
Saudi Arabia	800 814 0282
Saudi Arabia	800 850 0510
Serbia	0 800 190 167
Singapore	800-852-3912
Slovakia	0 800 002 487
Slovenia	0 804 88853
South Africa	080 098 3612
Spain	900 905460
Sri Lanka	247 2494
St. Lucia	1-844-236-5175
Sudan	15 655 9802



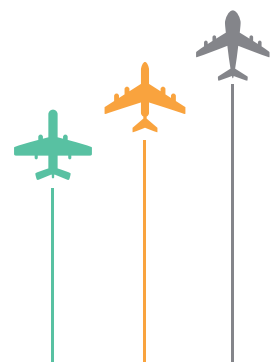
Puerto Rico	1 787 919 0326
Qatar	00800 100 801
Taiwan	00801 14 7064
Tanzania	0800 780 005
Thailand	1 800 012 657
Thailand (Bangkok)	2105 6161
Trinidad and Tobago	1-868-224-5814
Tunisia	31399185
Turkey	00-800-113-0803 90 850 390 2109
Uganda	206300115
Ukraine	0 800 501134
United Arab Emirates	8000 3570 3169
United Kingdom (includes England, Scotland, Northern Ireland, Wales)	0 808 189 1053
United States (includes US Virgin Islands, Puerto Rico, Guam)	1-800-461-9330
Uruguay	000 401 912 22

Sweden	020 889 823
Switzerland	0800 838 835
Uzbekistan	00 800 120 1246
Venezuela	0800 102 9423
Venezuela (Caracas)	212 720 2174
Vietnam	122 80 390
Vietnam (Ho Chi Minh)	2844581407
Zimbabwe	263 24 2799929
Note: For countries not listed here, use the following number. Operator assistance may be required and charges may apply.	+1 720 514 4400



Appendix 2: WFS Compliance Champions

Compliance Champion	Contact Email	Business Region / Location
France	whistleblowing.fr@wfs.aero	France CDG
Germany	whistleblowing.de@wfs.aero	Germany FRA
Spain	whistleblowing.es@wfs.aero	Spain MAD
United Kingdom	whistleblowing.uk@wfs.aero	United Kingdom LHR
Ireland	whistleblowing.ir@wfs.aero	Ireland DUB
Sweden	whistleblowing.se@wfs.aero	Sweden ARN
Denmark	whistleblowing.dk@wfs.aero	Denmark CPH
Netherlands	whistleblowing.nl@wfs.aero	Netherlands AMS
Belgium	whistleblowing.be@wfs.aero	Belgium BRU
Italy	whistleblowing.it@wfs.aero	Italy MXP
South Africa	whistleblowing.sa@wfs.aero	South Africa JNB
Thailand	whistleblowing.th@wfs.aero	Thailand BKK
Hong Kong	whistleblowing.hk@wfs.aero	Hong Kong HK
Singapore	whistleblowing.sg@wfs.aero	Singapore SIN
North America	whistleblowing.na@wfs.aero	USA DFW
Brazil	whistleblowing.br@wfs.aero	Brazil GRU
India	whistleblowing.in@wfs.aero	India BLR



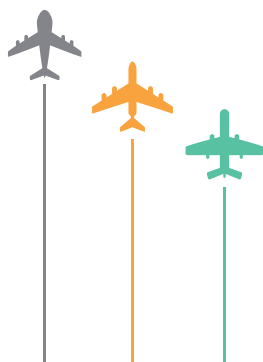
Appendix 3: Reporting Form

a) General Information:

- Name, Surname, and ID number of Whistleblower:
- Date of the report:
- Department/area of the Company to which the Whistleblower belongs (if an employee):
- Description of the relationship between the Whistleblower and the Company (if not an employee):
- Address or means of notification chosen by the Whistleblower (email, postal mail):
- Name and surname of the person(s) involved, and their communication data (if known):
- Dates of approximate moments of the occurrence of the reported events:
- Description of the reported events:
-

b) Type of infringement: (check with an x)

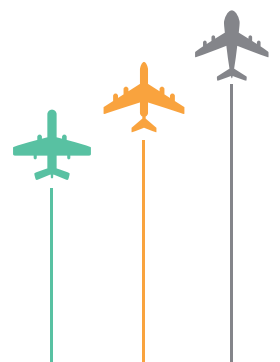
- Bribery
- Influence Peddling
- Business Corruption
- Fraud
- Discovery and Disclosure of Company Secrets
- Crimes against Personal and Family Privacy
- Breach and Falsification of Accounting Obligations
- Punishable Insolvencies
- Crimes against Intellectual Property
- Computer Damages, Cybercrimes
- Manipulation of Toxic, Corrosive, and other substances
- Crimes against Natural Resources and the Environment
- Crimes against Public Health
- Stock Market Crime
- Illegal Financing of Political Parties
- Violation of the Rights of Foreign Citizens
- Smuggling
- Money Laundering
- Terrorist Financing
- Organs Trafficking
- False Advertising
- Obstruction of Inspection Activity
- Other (please describe)



Appendix 3: Reporting Form

c) Considerations about the Alert reported:

- Detailed description of the reported events, including where they occurred, the possible person(s) involved or responsible, and the means used to carry out the events (if known).
- Description of the affected activity area, the possible relevant impact on the Company's work processes, whether or not it has an economic impact, and an approximate quantification (in euros).
- The communication must be as descriptive, specific, and detailed as possible, and should not contain offensive language.
- Attach supporting documentation or evidence of the reported events.
- The Whistleblower declares that the communication is made in good faith and that, except for unintentional errors or omissions, the data provided is true. The Whistleblower is also aware of the treatment that may be given to the personal data stated in this communication and the content of "Worldwide Flight Services' Whistleblowing Policy".
- This document will be kept in the Company's premises.



Appendix 4: Privacy Statement

1. Data Controller

WFS Global S.A.S.

2. DPO

dpo@wfs.aero

3. Lawful basis for personal data processing

The lawful basis WFS relies upon to process personal data is in compliance with the relevant legal obligations set up by the Directive (EU) 2019/1937, its national transposition laws and any other national applicable laws.

If the personal data that WFS receives contains special categories of data such as but not limited to health, religious or ethnic affiliation, or if it is not necessary for the handling of the report, WFS will refrain from collecting it or, if accidentally collected, WFS will ensure its deletion.

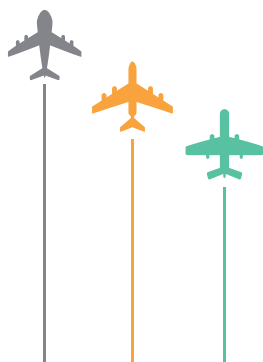
4. Data Protection principles

The following principles guide WFS' processing of personal data:

- WFS is committed to handling personal data in a manner that is lawful, fair, and transparent.
- Personal data will be processed only for the purpose of investigation and addressing the reported concern.
- WFS will take reasonable measures to ensure that personal data is accurate and up-to-date. Any inaccurate or incomplete data will be promptly corrected or deleted. Personal data that falls outside the scope of this Policy will be immediately deleted. Security: adequate technical and organizational measures will be taken to ensure the security of personal data. These measures will be appropriate to the risks presented by the processing and the nature of the personal data being processed.

5. Data Subjects

- Whistleblower - the individual who reports or alerts about concerns deemed reportable under this Policy.
- In cases where the report is made anonymously, personal data protection regulations would not apply to the Whistleblower. However, WFS will adopt appropriate measures to ensure maximum confidentiality.
- WFS has implemented technical and organizational measures to protect the Whistleblower and ensure the confidentiality of data relating to any individuals investigated based on the report.
- Reported Party - the person to whom the reported infringement is attributed or with whom the infringement is associated.
- The same rules laid down for the protection of the Whistleblower's identity will apply equally to the protection of the identity of the reported party.



Appendix 4: Privacy Statement

- Third parties - such as but not limited to the witnesses or co-workers. Any processing of third party's personal data will be limited to what is necessary for the purpose of investigating and addressing the reported concern. WFS will take reasonable measures to ensure the accuracy and completeness of third-party personal data and will delete any data that is no longer necessary or relevant for the investigation.

6. Categories of personal data processed

WFS will process any personal data provided by the Whistleblower within their report.

7. Disclosure of personal data

To ensure the protection of personal data, WFS guarantees strict access control measures for personal data, limiting access only to those individuals who have a legitimate right to access such data based on their assigned responsibilities under this Policy.

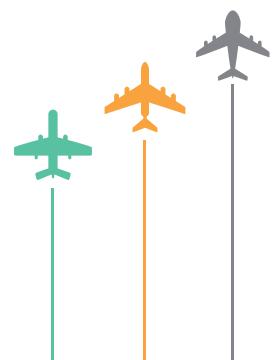
A limited number of designated persons, who are specially authorized WFS employees, will collect and process the Alerts. They are subject to strict duties of confidentiality, impartiality, transparency, and loyalty towards the persons whose data is processed as part of the Alert. In the performance of their duties, they report to the Compliance Officer who carries out his/her mission under the supervision of the Group General Counsel.

The information collected in the report may be disclosed on a need-to-know basis to external advisors of WFS, such as legal, auditing, finance and accounting, information technology and human resources advisors or similar consultants and advisors, who are bound by the same confidentiality requirements to the extent permitted by applicable law.

In circumstances where personal data is disclosed in the context of an investigation or under an administrative or criminal proceeding, such as to the Judicial Authority, the Public Prosecutor's Office or the Administrative Authority, WFS will ensure that the legal provisions are in place to protect the identity of the persons whose data is processed as part of the Alert.

8. Duration for which personal data is kept

WFS will retain personal data for the time necessary to investigate and address the reported concern. If no investigation is initiated within (3) three months of receipt of the Alert, WFS will delete the information, unless it is required to be retained for a longer period to comply with the legal or regulatory requirements. In exceptional cases where the data must be retained, it will be anonymized, to protect the identity of the individuals involved.



9. Security safeguards

- Access to personal data is strictly controlled, limited to those individuals who have a legitimate right to access the data for their assigned responsibilities under this Policy.
- WFS has contracted CONVERCENT as a trusted personal data processor to host and administer the Ethics Hotline. CONVERCENT has implemented appropriate technical, organizational and administrative security measures to protect the personal data it processes on behalf of WFS.
- WFS stores archived data in a separate, secure system to further ensure the confidentiality and security of the personal information.
- Our technical safeguards are designed to ensure the integrity, availability, and confidentiality of the personal information that is processed.

10. International Transfers

WFS will not transfer any personal data collected to countries outside of the European Economic Area (EEA) or to countries that are not considered by the European Commission to providing an adequate level of data protection without having implemented the required protection instruments ahead of the transfer.

11. Data protection rights

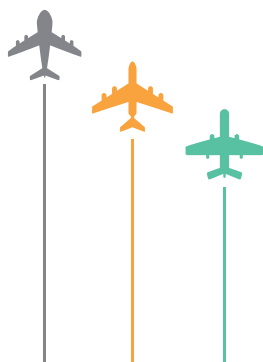
Data subjects have the right to access, request corrections, delete, and restrict the processing of their personal data, as well as the right to object to such processing. To exercise any of these rights, please contact dpo@wfs.aero.

While WFS will make every effort to fulfil the requests, the Company may have valid reasons not to comply with your request if it would jeopardize an investigation. For example, if the Whistleblower did not provide sufficient contact details or if fulfilling the request could compromise an ongoing criminal investigation.

If the data subject believes that their data protection rights have been violated, they also have the right to file a complaint with the local supervisory authority.

WFS may update this Privacy Statement from time to time to reflect changes in this Policy or to comply with the legal obligations. We encourage all persons acting under the scope of this Policy to review this Privacy Statement periodically.

If there are any questions or concerns about this Privacy Statement or our Policy, please contact us at dpo@wfs.aero.



Appendix 5: Definitions

Alert

The act of reporting a concern or suspicion of unethical, illegal, or non-compliant behaviour within an organization. It is a mechanism for employees or other individuals associated with the organization to report any wrongdoing without fear of retaliation.

Data Subject

An “identified or identifiable natural person” from whom or about whom information is collected. A company or organisation cannot be a data subject.

DIRECTIVE (EU) 2019/1937

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.

GDPR

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation).

Special Categories of Data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

WFS Compliance Officer

Responsible for overseeing and ensuring the Company's adherence to the highest ethical standards and all applicable laws and regulations, including but not limited to Anti-corruption, Trade Sanctions, and internal policies and procedures. Accountable for the design and correct implementation of WFS Compliance Program.

WFS Compliance Champion

Responsible for ensuring the correct and effective deployment of WFS Compliance Program at local level, and to serve as the main local touchpoint for compliance-related issues or concerns.

WFS Compliance Program

Refers to the set of internal policies and procedures that are currently in effect at WFS with the primary objective of preventing, detecting, and responding to acts or behaviours that may violate legal or regulatory requirements, corporate policies or ethical standards. Its ultimate goal is to ensure that WFS complies with all relevant laws and regulations, and that its operations align with the highest ethical standards and values. It includes, among others, this Policy, WFS Code of Conduct, WFS Anti-corruption Policy, WFS Trade Sanctions Policy and WFS Operating Procedure.

