SMALL WORLD FINANCIAL SERVICES GROUP

WHISTLEBLOWING CHANNEL POLICY

Hereinafter, the "SWFSG".

1st version	November	2016
2nd version	January	2017
3rd version	November	2019
4th version	September	2020
5th version	April	2021
6th version	June	2023

Information Classification: Internal.

Access: **Access** granted to all employees, suppliers, clients, vendors or contractors of Small World. Only the corresponding Compliance Officers for each country may authorise access to external parties.

Copy: Only authorised personnel (Access) may create physical and digital copies of the document. Storage: Physical copies shall not be left visible when unattended. Logical storage shall adhere to the access restriction rules.

Transmission: Authorised personnel shall only share the document to previously authorised recipients using encrypted channels or at least file encryption. Keys and/or passwords will never be shared through the same channel. Physical copies will be delivered to the recipient and sent via a secure mail service if necessary.

Destruction: Hard copies shall be disposed of using a shredder. Logical destruction of copies shall be carried out by any authorised party after the end of life (end of use) of the copy. The document shall be completely destroyed as instructed by the Legal Department.

1. Overview and objective

This policy sets out the main guidelines and procedures for handling allegations against the Small World Financial Services Group of Companies (hereinafter referred to as "SWFSG") concerning compliance with its obligations in terms of ethics and good governance.

SWFSG must respond adequately to the allegations of all whistleblowers, protecting the ones who come forward in good faith from retaliation and also ensure that all parties affected by the allegations have the opportunity to present relevant evidence to explain or defend themselves and understand the nature of the allegations.

2. Legislation

Adopted as *Directive 2019/1937*, the EU Whistleblowing Directive entered into force in November 2019. Member States had to harmonise their own legislation by 17 December 2021. While this Directive does not apply to the UK, the UK Government nevertheless has the *1998 Public Interest Disclosure Act* (PIDA) providing for similar conditions.

This legislation is particularly relevant in terms of data protection, including the protection of whistleblowers reporting breaches at SWFSG.

It should be noted that the Directive significantly broadens the scope of whistleblowers. Suppliers, former employees, customers, etc. and any other stakeholder may be potential whistleblowers.

In addition to the above legislation, SWFSG, as a group of payment institutions, must also adhere to the anti-money laundering and/or anti-terrorist financing requirements set out in the Anti-Money Laundering and Terrorist Financing Directive (*AMLD IV*). The necessity for a Whistleblowing Channel appears as an essential element of the Compliance and Regulatory Risk Prevention Models, according to which whistleblowing channels must permit anonymous whistleblowing.

Finally, there is specific legislation at the local level in the jurisdictions affecting SWFSG that should also be observed:

- GDPR, Schrem's II and global data privacy legislation
- Section 301 of the U.S. SOX Act on corporate responsibility
- German Government Corporation Code
- French Sapin II Act

3. Core policy principles.

The core principles guiding the present policy are:

- Accessibility
- Transparency
- Good faith
- Whistleblower protection
- Confidentiality
- Objectivity and impartiality
- Conflict of interest
- Prohibition of retaliation

- Right to defence

In all cases, whistleblowers shall have the following rights:

- Right to be informed about the availability of the channel.
- Right to confidentiality
- Right to remain anonymous
- Right to personal data protection
- Right not to face retaliation
- Right to be informed of the resolution or closure of the communication

Whistleblowers shall also have the following obligations:

- Act in good faith
- Provide data and documents related to the alleged facts.
- Duty to safeguard confidentiality

The reported party shall always be entitled to the following rights:

- To be notified as soon as possible that he or she is under investigation because of allegations against him or her. This notification must contain information on the management body handling the allegations, and the reported party's corresponding rights.
- Allegation handling procedure.
- Right to access data on file, with the exception of the identity of the whistleblower and anyone else concerned by the file.
- Right to rectify any incorrect or incomplete personal data.
- Right to be informed of the resolution or closure of the communication

4. Purpose and Scope of the Policy

This Policy was drawn up to enhance the obligation to use the SWFSG Whistleblower Channel, and define and clarify how it may be used, thus providing advice and certainty in the decision-making process of anyone witnessing potential system violations.

In keeping with the legislation referred to in the previous section, SWFSG intends to establish a clear principle:

Retaliation on account of having lodged an allegation is prohibited in the SWFSG and, for this purpose, the following key issues need to be determined:

4.1. Subjective scope of application: who is covered by this policy?

This policy covers:

a) All SWFSG employees

(b) Self-employed individuals under contract for the provision of services with an SWFSG company.

(c) shareholders and anyone serving as a member of the administrative, management or supervisory body of SWFSG, including non-executive members, volunteers and paid or unpaid trainees/interns.

(d) anyone working under the supervision and direction of Small World, subcontractors, vendors, service providers and suppliers.

(e) any other stakeholder may also be considered to be a potential whistleblower

4.2. Objective Scope of application: What can be reported?

This Policy encourages disclosure of any concerns that the whistleblower may have regarding possible violations of SWFSG Policies and applicable laws in any jurisdictions where SWFSG operates, in accordance with the breadth defined in Directive (EU) 1937/2019 and related implementing legislation. This includes information on breaches broadly defined, i.e. reasonable concerns or suspicions, actual or potential breaches, whether they have occurred or are likely to occur.

In this regard, the following communications are possible:

a) Offences against the rights of foreigners
b) Workplace harassment (physical, psychological, sexual harassment and cyber-bullying)
c) Hacking into computers to steal sensitive personal data
d) Concealing assets and criminal insolvencies
e) Money laundering and financial crime
f) Data security breaches ("data breaches") (misuse of personal data belonging to the company)
g) Collusion with competitors
h) Conflicts of interest
i) Crimes against the environment
j) Crimes against the Public Treasury and Social Security
k) Crimes of drug trafficking against public health
l) Corruption and bribery
m) Crimes against workers' rights
n) IT system damage
o) Crimes related to Industrial Property, Intellectual Property, Market and Private Corruption
p) Disclosure of trade secrets
q) Scam, fraud
r) Counterfeiting of credit and debit cards and travellers' cheques
s) Falsification, alteration or substitution of company records
t) Incitement to hatred and violence
u) Inaccuracy of ledger books and records
v) Breaches of consumer protection law
w) Breaches of the SWFSG Code of Conduct
x) Misappropriation of funds
y) Obstruction of inspection or monitoring activity
z) Organisations and criminal groups

aa) Internal business practices inconsistent with GAAP
bb) Influence peddling
cc) Degrading treatment, acts against moral integrity, repeated hostile or humiliating acts.
dd) Insider information
ee) Infringement of confidential information and trade secrets

5. Procedure

Anyone referred to in section 2 (Scope of application) who suspects serious breaches of Company policy or the law, should report them immediately, anonymously or by identifying themselves, through the digital whistleblowing channel available on the Small World website at the following link:

https://whistleblowersoftware.com/secure/smallworldcanaldedenuncias

This channel can also guarantee the anonymity of the whistleblower, if preferred.

All issues or breaches will be properly resolved through this channel in accordance with the Whistleblower Channel Protocol, which is also available on the Small World website.

The individuals responsible for managing compliance will be:

Group status	Country	Categories
Compliance Officer	Belgium	Everything, except abuse
Compliance Officer	Portugal	Everything, except abuse
Compliance Officer	UK	Everything, except abuse
Compliance Officer	Italy	Everything, except abuse
Compliance Officer	UK	Everything, except abuse
Compliance Officer	Switzerland	Everything, except abuse
Compliance Officer	Chile	Everything, except abuse
Compliance Officer	USA	Everything, except abuse
Compliance Officer	Africa	Everything, except abuse
Compliance Officer	Sweden, Norway, Finland, Denmark	Everything, except abuse
Compliance Officer	Brazil	Everything, except abuse
Compliance Officer	France	Everything, except abuse
Compliance Officer	Spain	Everything, except abuse
Compliance Officer	The Netherlands	Everything, except abuse
Compliance	Ireland	Everything, except abuse

Officer		
Global Compliance Officer	Canada	Everything, except abuse
Global Compliance Officer	Greece, Cyprus	Everything, except abuse
Compliance Officer	Germany	Everything, except abuse
RPD	Group	Everything, except abuse
Legal Risks	Spain, Chile, Brazil, Italy, Portugal, Greece, Cyprus	Everything, except abuse
Legal Risks	USA	Everything, except abuse
Legal Risks	UK	Everything, except abuse
HR	Spain, Chile, Brazil	Abuse
HR	Group	Abuse

What information should I provide as a whistleblower?

SWFSG hopes that your information will be as thorough and truthful as possible. We therefore ask whistleblowers to disclose all the information known to them about possible breaches. And to do so in detail. It is also preferable to submit evidence or documents supporting the allegations, which should refer to this evidence and documents. Doing so will enable SWFSG to manage the case as quickly and efficiently as possible.

Whistleblower identification when reporting: Anonymity

The SWFSG's Whistleblower Channel has been designed to allow anonymous reporting.

However, SWFSG recommends that whistleblowers identify themselves by name, job title and contact details when submitting allegations. The personnel in charge of handling the matter will then be able to contact the whistleblower to follow up if necessary. SWFSG also sees this as the best way to demonstrate its policy of non-retaliation towards whistleblowers.

In this regard, when a (non-anonymous) report is filed, SWFSG ensures that the corresponding internal procedure will be conducted in a secure manner so as to safeguard the confidentiality of the whistleblower's identity and other related information.

What happens when filing a report through the SWFSG Whistleblowing Channel?

SWFSG uses a digital platform compliant with the requirements of Directive 1937/2019.

Reports through this digital channel are stored directly on the platform, which has implemented robust information security measures aimed at preserving the integrity, availability and confidentiality of the information.

The platform gives the whistleblower the opportunity to specify the place, date, company or Division concerned, and also the persons involved in the alleged breach. It also allows for the option of anonymous communication. The platform will also give the whistleblower an option to attach supporting documentation to the communication to justify the content of the allegation or report.

The Regulatory Compliance Division at SWFSG will acknowledge receipt within seven days.

Following acknowledgement of receipt, if the whistleblower has identified him/herself, SWFSG may have an internally designated person, referred to as the Case Manager, contact the whistleblower directly to identify him/herself as the investigator, and provide feedback and updates. Allegations will be processed within a reasonable period of time, not exceeding three (3) months from the acknowledgement of receipt, which may be extended to six (6) months in cases of special relevance or complexity. However, after the first three months from the receipt of the allegation, any information of a personal nature concerning the whistleblower, the reported persons or third parties shall be removed from the whistleblower channel, unless it is essential to keep it as evidence that the crime prevention model works.

It is essential to note that the platform passes allegations only to specific individuals within the SWFSG who are authorised to handle them. The in-house team handling the submitted documents also receives training on how to effectively manage and ensure the confidentiality of the documents and allegations.

The principle of action is that, where the allegation indicates a possible violation of the SWFSG Global Compliance Management System, an investigation will be initiated in accordance with the "SWFSG Whistleblower Channel Procedure".

SWFSG will inform the whistleblower of the allegation and, to the extent possible, of the outcome of the assessment of the case. Please note that there are limitations to the updates that can be provided on the allegation, subject to the aforementioned "SWFSG Whistleblower Channel Procedure".

Fair and responsible handling of allegations

The company is also bound by the principle of good faith. SWFSG therefore observes the rights of employees and ensures that the rights of employees identified in allegations made are also protected in accordance with this Policy.

Prohibition of retaliation

SWFSG tolerates no form of retaliation whatsoever. This includes threats, or any other means of intimidating a whistleblower who makes a bona fide allegation in connection with this Policy.

What is meant by good faith in terms of the company and whistleblower?

Good faith with regard to the whistleblower presumes that the whistleblower has at least reasonable grounds to believe that the information about possible infringements reported was true when the allegation was filed.

Good faith means that the company will not retaliate in any way for making an allegation, and will protect confidentiality, with the following exceptions only:

a) Whenever the law, in its different modalities, stipulates that it must be communicated to a judicial or administrative authority.

b) Whenever it is essential with regard to external advisors and consultants and other SWFSG suppliers to operate the Whistleblower Channel or to investigate the allegations, as set out in this policy. In such cases, SWFSG contractually stipulates confidentiality from these third parties.

What does the prohibition of retaliation mean?

The prohibition of retaliation covers any act or omission, direct or indirect, that may harm a whistleblower because of his or her good faith allegation of a possible wrongdoing.

For instance, SWFSG will take none of the following actions against whistleblowers for filing an allegation:

1. Suspension, dismissal, redundancy or equivalent measures;
2. A negative performance assessment
3. Denial of promotion;
4. Unjustified change of workplace location, salary reduction,
change in working hours;
5. Coercion, intimidation, harassment or ostracism;
6. Discrimination, disadvantageous or unfair treatment;
7. Non-renewal or early termination of a temporary employment contract;
8. Harm, including reputational harm, particularly on social media,
or financial loss, including loss of business and loss of income;
9. Early termination of a contract for goods or services;
10. Cancellation of a permit,
11. Among other measures that could be considered retaliatory.

The prohibition of retaliation in case of external allegations and public disclosures

Protection against retaliation also extends to anyone who makes allegations of possible breaches externally to the competent authorities.

Both direct and indirect reprisals are prohibited.

The prohibition of retaliation herein also covers the following persons:

1. any third party related to the whistleblower (such as co-workers and family members) who may face retaliation in an employment context;
2. anyone who has helped the whistleblower in the allegation process;
3. any legal entity that the whistleblower owns, works for or is otherwise connected with in an employment or professional context.

Should any person at SWFSG directly or indirectly retaliate in violation of this Policy, ACS will take the necessary steps to ensure that the retaliation ceases as soon as possible and, where appropriate, take disciplinary action against the party responsible for the retaliation.

6. Data protection and retention

Identity of the data controller

The personal data of the whistleblower will be processed by the SWFSG entity to which the allegation is addressed.

SWFSG undertakes to rigorously safeguard the data privacy, security and retention, as further specified in our Compliance policies and procedures. These rules will also apply in respect of all personal data relating to allegations made in accordance with this Policy.

Personal data retention

SWFSG will keep a record of all allegations received. These records and the personal data contained therein shall be kept confidential. Records shall be kept for no longer than is necessary and in any event for as long as is necessary to comply with any applicable legal requirements at all times.

In particular, SWFSG will retain the whistleblower's personal data for the time necessary to decide whether to initiate an investigation into the allegations or conduct and, once decided, the data will be deleted from the Whistleblower Channel but may also be processed outside the system to investigate the allegations for the time necessary to reach a decision. Once the investigation of the allegation has been completed and any appropriate measures have been taken, if necessary, the data of those allegations that have been followed up will be duly blocked to comply with the corresponding legal obligations in each case.

In any case, personal data will be deleted from the Whistleblower Channel after three (3) months have elapsed since they were entered, unless they must be retained for a further period of time to comply with legal and corporate obligations or to provide evidence that the crime prevention model works properly. They may, however, continue to be processed outside the Whistleblower Channel if the investigation thereof has not concluded, for as long as necessary until its conclusion.

Should a decision be taken not to pursue the allegation filed, the information may be rendered anonymous and retained.

What personal data does SWFSG collect?

In handling allegations made in accordance with this Policy, SWFSG collects the following personal data and information provided when making an allegation and throughout the investigation of the allegation:

- Whistleblower name and contact particulars (except anonymous allegations) and whether the whistleblower is an SWFSG employee
- Name and other personal particulars of parties named in the allegation (alleged offender, possible witnesses and others), when such information is provided (i.e. job description, contact details and involvement or role with respect to the allegations);
- Description of the alleged breach and circumstances regarding the incident or incidents.
- Any other documentation that the whistleblower wishes to attach to the allegation that may contain personal data.

For what purpose does SWFSG process personal data?

SWFSG only processes personal data that are strictly necessary for handling, processing and investigating allegations of wrongdoing or acts contrary to the ethics, legality or corporate rules of the SWFSG Group. This includes the necessary steps to investigate the allegations, including, where appropriate, the necessary disciplinary or legal action.
Personal data will only be used for the aforementioned purpose and never for any other purpose.

What is the legal basis for the processing?

Personal data processing within the framework of the internal communications channel is contemplated in Articles 6.1.c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016; 8 of Spanish Law 3/2018 of 5 December; and 11 of Spanish Law 7/2021 of 26 May, which stipulates a statutory internal reporting system.

If it is not compulsory, the processing shall be presumed to be covered by Article 6(1)(e) of the EU Regulation cited above.

Personal data processing in the cases of external communication channels shall be considered lawful as provided for under Articles 6.1.c) of Regulation (EU) 2016/679; 8 of Spanish Law 3/2018 of 5 December; and 11 of Spanish Law 7/2021 of 26 May.

Should the whistleblowing system render the processing of special categories of personal data necessary for reasons of essential public interest, this processing may be carried out in accordance with Article 9(2)(g) of Regulation (EU) 2016/679.
Processing the whistleblower's personal data is therefore strictly necessary to manage the allegation and comply with the aforementioned purposes and legal obligations. SWFSG will in no case make automated decisions based on the data submitted.

Who are the recipients of the personal data?

Personal data collected in the context of allegations filed through alternative whistleblowing channels may be processed or disclosed to the following parties where necessary:

- The platform service provider that manages the alternative whistleblowing channels on a daily basis.
- Members of the SWFSG Compliance Committee.
- Authorised agents of SWFSG, provided that the nature or extent of the allegations requires their involvement.
- External investigator, consultant or advisor who has been engaged to assist SWFSG in the assessment of the notification or investigation of the matter, or to advise SWFSG therein.
- Police and/or other regulatory or law enforcement authorities.

What are the whistleblower's data protection rights?

As an informer, the whistleblower making the allegation may exercise, at any time and under the terms provided for by the pertinent legislation and regulations in force, the right to access the personal data concerning him/her as data subject. If this data subject believes that the data are incorrect or incomplete, he or she may request their rectification in accordance with the applicable legislation.

The data subject may thus request erasure of the data when they are no longer needed, except in cases where there is a legal obligation to retain them. The data subject may also request the

portability or restriction of processing, or object to the processing of, his or her data, and shall have the right to withdraw his or her consent in this regard. When filing an allegation, whistleblowers shall be informed how to exercise all these rights.

Whistleblowers may also lodge a complaint with the competent data protection authority whenever deeming it appropriate to do so.

Where can I get more information on personal data processing concerning me?

You can get further information about the processing of your personal data and contact particulars of the possible entity agent assigned for this purpose, Data Protection Officer or other privacy officer. When filing an allegation, whistleblowers will be informed on how to obtain this information.

7. Policy approval requirements

This policy shall be revised, updated, if necessary, and re-approved by the Compliance Committee at least every 12 months.

8. Implementation of established policies and procedures

Senior management in each country is ultimately responsible for ensuring compliance with the policy within their organisations. Failure to comply with established policies or procedures constitutes a breach of the terms and conditions of employment and may result in disciplinary action, up to and including dismissal.