HSBC

HSBC Whistleblowing Arrangements in Greece

HSBC's 'Speak-up'_culture, as part of the Conduct Framework, encourages our people to raise concerns in confidence without fear of any form of retaliation through our HSBC Confidential Whistleblowing Channel. As well as employees, HSBC also welcomes concerns raised by any Eligible Person.

Who is an Eligible Person who can raise a concern using HSBC Greece Whistleblowing arrangements?

You can raise a whistleblowing concern to HSBC if you are:

- an HSBC employee
- an ex-employee, as long as the information you report was collected when you worked at HSBC
- being hired, as long as the information you report was collected during your hiring
- an intern of HSBC
- a volunteer at HSBC
- a leader at HSBC
- a shareholder or HSBC partner
- an external or occasional collaborator with HSBC, such as a consultant
- a supplier to HSBC
- a subcontractor or co-contractor
- someone with general meeting voting rights
- a member of the administrative, management or supervisory body of any HSBC entity in Greece

Scope of the Whistleblowing arrangement

The Whistleblowing arrangements allows you to raise concerns about:

- a crime or misdemeanor, such as corruption, fraud and embezzlement, harassment, discrimination, etc.
- a breach or attempted concealment of a breach of any international standard, law or regulation
- a threat or harm to the public interest
- an attack on human rights and fundamental freedoms, the health and safety of people and the environment, resulting from the activities of HSBC in Greece, as well as those of its subcontractors or suppliers
- any situation which could generate a significant financial or reputational risk for the bank. Reports in this category will be reviewed on a case-by-case basis to determine whether or not they should be processed via the alert system.

In addition, as per Greek law the following breaches can be reported:

- breaches falling within the scope of EU Law that concern the following areas: (i) public procurement, (ii) financial services, products and markets and prevention of money laundering and terrorist financing, (iii) product safety and compliance, (iv) transport safety, (v) protection of the environment, (vi) radiation protection and nuclear safety, (vii) food and feed safety, animal health and welfare, (viii) public health, (ix) consumer protection and (x) protection of privacy and personal data and security of network and information system.
- Breaches relating to fraud or any other illegal activities affecting the financial interests of the EU and
- Breaches relating to the internal market, as referred to in Art. 26 (2) TFEU (free movement of goods, persons, services, and capital) including infringements of competition law rules, state aid rules and corporate tax rules.

To illustrate, the whistleblowing concerns, may include, but are not limited to:

- inappropriate personal behavior
- market abuse
- mistreatment of a client
- fraud
- theft
- corruption
- non-compliance with competition law
- creating a dangerous working environment
- intimidation and harassment
- discrimination and concealment of facts or misconducts

If HSBC Confidential is not the most appropriate channel to deal with your report, we may discuss the matter with you and redirect your concern to an alternative channel.

Investigations

Reported concerns will be subject to internal investigation conducted by independent and competent experts. At the end of the investigation, we will provide you with as much feedback as we can about the outcome of the case.

Anonymity

You can raise concerns anonymously, but we encourage you to provide contact details to help us complete our investigation more easily and thoroughly.

Confidentiality

All cases are logged and treated confidentially, with your identity only accessible by the relevant HSBC Confidential team and those who are involved in investigating your concern. We will only disclose your identity where we are required to for legal or regulatory reasons.
Information that could identify you will only be disclosed with your permission, unless we are legally required to share such information in case of legal proceedings.

Sometimes, it may not be possible for us to conduct our investigation without revealing your identity. If this is the case, we will discuss it with you and make sure you agree before moving forward.

Protection

You can always raise a whistleblowing concern safely, without fear of retaliation. To receive protection under Greek legislation, whistleblowing concerns must be raised in good faith and without direct financial compensation.

Data protection

The HSBC Confidential Whistleblowing Channel complies with the provisions of the EU General Data Protection Regulations (GDPR).

How to raise a Whistleblowing Concern?

If you are an eligible person, you can raise your concerns in 3 ways:

A. You can use the internal whistleblowing channel, HSBC Confidential:

1. By Completing an online form.

To avoid any compatibility issues, please use a Microsoft Edge or Google Chrome internet browser when submitting your report. If you want to remain anonymous you can provide an email address, which will be encrypted and it will not be disclosed to HSBC. Encrypted email addresses will be used to facilitate communication between the Whistleblower and HSBC.

2. By Phone through our 24/7 Line.

If you make your report orally, during the call you can ask for a video or physical meeting. It must take place within a reasonable time after we receive your request.

Please note that the above 2 methods for raising concerns are hosted by NAVEX Global, an external third party. The link to the Navex portal can be found **here.**

3. To the Greece Responsible Officer.

Reports raised directly to the Greece Responsible Officer can be submitted in writing (e mail , letter , Executive Referral) or orally. Verbal reports can be submitted via telephone either via local recorded line 0030 210 6961104 (Monday to Friday 10:00 - 16:00), as well as through a personal meeting with the Responsible Officer within a reasonable time, at the request of the reporting person.

The Greece Responsible Officer is: Constantina Tyrovoli , Chief Compliance Officer, HSBC Greece (hsbc-confidential-greece@hsbc.com)

The delegated Responsible Officer is: Christina Krikelaidou, Compliance Manager, HSBC Greece (hsbc-confidential-greece@hsbc.com)

B. You can use External Channels established by Public Authorities

HSBC encourages you to use our internal whistleblowing channels before going to any external channels set up by public authorities. However, you are not precluded from using an external channel first.

C. You can make a Public Disclosure (making information on breaches available in the public domain (especially in media and websites).

A person who makes a public disclosure shall qualify for protection if any of the following conditions is fulfilled:

i. the person first reported internally - to the Responsible Officer or the Integrity Consultant - or directly externally to the National Transparency Authority, but no appropriate action was taken in response to the report within the set time frame;
ii. the person has reasonable grounds to believe that the breach may constitute danger to the public interest, or there is an emergency situation or a risk of irreversible damage, or in the case of external reporting to the National Transparency Authority 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.

Personal Data

However, you choose to raise your concerns with us, the information we collect will be kept confidential at all times. To see how we process your personal data through HSBC Confidential, check the HSBC Continental Europe Greece Privacy Notice available in Public Website & the PRIVACY NOTICE GREECE - NOTICE ON THE OPERATION OF THE INTERNAL REPORTING CHANNEL & THE RELEVANT PROCESSING OF PERSONAL DATA which is available in the Terms & Conditions and Privacy statement. This Privacy Notice applies to all personal data processed by entities of the HSBC Group acting as data controllers. It explains how we use this data, who we share it with and what steps we take to ensure its confidentiality and security.