HSBC CONFIDENTIAL

Terms and Conditions and Privacy Statement HSBC Confidential is the HSBC whistleblowing channel. This document provides important information relating to the use of HSBC Confidential. Please take the time to read this information.

General Use

HSBC Confidential is operated by Whistleblowing Oversight Teams within Compliance and is subject to all of the rules held within this document.

Please note local data sharing restrictions may exist in your country which prohibit the disclosure of sensitive client information. This may include but is not limited to: clients name, address, account reference, account number, any other client identifying data. Therefore, please do not share client information, or disclose any Material Non-Public Information or other commercially sensitive information through HSBC Confidential. Furthermore, please do not use the HSBC Confidential channel to share Suspicious Activity Reports (SAR) or any SAR related data.

When raising a case through HSBC Confidential, your data may be collected by NAVEX Global, a third party to the HSBC Group. The relevant data privacy statement can be found on the NAVEX Global web portal.

After raising your concern through HSBC Confidential, please do not raise it via any other internal channel as this may delay the investigation process.

Your concern will be impartially investigated in an appropriate and timely manner by relevant subject matter experts. If the team handling your concern does not think HSBC Confidential is the most appropriate channel, an alternative route may be recommended. All concerns are logged and treated confidentially as far as possible. All identifying details are securely maintained with access controls in place to confirm only authorised staff handling your concern have access. You are encouraged to provide identifying details as this may help to facilitate the investigation and the level of feedback able to be provided at the conclusion of a case.

All information relating to a HSBC Confidential case will be kept confidential to protect the identity of individual submitting the report and the subject of the report. There are limited exceptions to the general requirement for confidentiality where there is good reason to disclose, for example when required by law or regulation.

Privacy Statement

In raising a concern via the HSBC Confidential channel you acknowledge that any data you provide will be processed and handled for the purposes of the investigation. Any personal data you provide will be kept confidential and processed in accordance with applicable data privacy laws and the HR Data Privacy Notice which can be found on HR Direct (if applicable within your jurisdiction).

The information you provide may be shared with other HSBC group entities including across borders to jurisdictions which do not have data protection laws providing the same level of protection as the jurisdiction in which you are based. The information may also be shared subject to applicable data privacy laws, with any sub-contractors, agents, advisers or service providers of the HSBC group (including their employees, directors and officers) as well as any regulatory authorities of the HSBC group.

The information provided will be kept confidential and protected by appropriate security and technical measures at all times. The data controller in relation to the information you provide is the HSBC group entity which is conducting the investigation into your concern. Information provided in a report will be kept in accordance with existing records retention schedules for the relevant HSBC group entity.

In certain jurisdictions, data privacy laws may allow you to make a written request for a copy of the personal data we hold about you and to ask us to rectify, erase or block any inaccurate data. You should make a request to the HSBC group entity which is conducting the investigation and will be able to direct your query.

Management Reporting of Whistleblowing Cases

Aggregated data from concerns raised through HSBC Confidential is used in presentations and governance reports for management information purposes. Data is collected and collated securely to ensure that the identity of the person who raised the concern is always protected and anonymised. This means that where cases are used in any reports, nothing that may reveal your identity will be disclosed. Board reports provide aggregated data, for example the total number of HSBC Confidential cases from various regions in which HSBC operates, the categories of concerns, and management information on trends. Where specific details of cases warrant the attention of the Board; the cases are also anonymised.

II. LOCAL POLICY GREECE (LAW 4990/2022 FOR THE PROTECTION OF WHISTLEBLOWERS)

1. Scope: The scope of this policy is to cater for the local requirements mandated by the Greek Law 4990/2022 for the Protection of Whistleblowers ("the Law").

2. According to the Law the following breaches can be reported:

- **a.** 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.**

b. Breaches relating to fraud or any other illegal activities affecting the financial interests of the EU and

c. 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.**

Certain EU legislation is stated in the Appendix attached to Law 4990/2022.

3. Procedure of submission of reports: Reports can be submitted by persons working in the private (or public) sector, who acquired information on or observed violations of EU law in their work-related activities. That said, **Whistleblowers/Reporters can be:** employees of the Bank (full or part-time, indefinite or fixed term, posted, etc.); self-employed persons, consultants and home workers; shareholders and persons belonging in the administrative, management or supervisory bodies of the Bank, including non-executive members, as well as volunteers and paid or unpaid trainees; any person working under the supervision and direction of contractors, subcontractors and suppliers etc. Furthermore, the Law applies to any person who reports or publicly discloses information on EU law violations, which they acquired in the context of a work-based relationship which has ended (in any way, including retirement) or is yet to begin (e.g., during the recruitment process or other pre-contractual negotiations).

The measures for the protection of reporting persons shall also apply to:

• facilitators;

• third persons - such as colleagues or relatives of the reporting persons - who are connected with the reporting persons and who could suffer retaliation in a work-related context; and

• legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context

4. Anonymous reports: The Law allows anonymous reports, as it provides that anonymous reporting persons will enjoy protection, if they are identified at a later stage and if retaliation measures would apply. The Law does not specify any particulars as to when or how they shall be identified, and in its current form it does not provide any other clarifications as to anonymous reporting.

5. Reporting persons shall qualify for protection under the Law provided that: (a) they had reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of the Law; and (b) they reported either internally or externally in accordance or made a public disclosure or applied directly in appropriate EU bodies and organizations.

6. Internal Report Procedure: The internal report is submitted in writing (e mail, letter, Executive Referral) or orally or through an electronic platform which operates on the website and the intranet of HSBC (HSBC Confidential). The verbal report can be submitted via telephone either via local recorded line 0030 210 6961104 (Monday to Friday 10:00 - 16:00) or via NAVEX call center (HSBC Confidential, 24x7) as above as well as through a personal meeting with the Responsible Officer within a reasonable time, at the request of the reporting person.

7. HSBC's local Whistleblowing Responsible Officer for HSBC Greece- 'Bank' is responsible for receiving any reports via the local recorded line and re direct to HSBC Global Whistleblowing Team (HSBC Confidential) in order to take all required actions in the conduct of any required

investigations along with Greece Responsible Officer oversight. This includes performing a preliminary review of reports received from any person who is able to make the disclosure in accordance with the Law and assigning the report for investigation. The Responsible Officer should have direct, unfettered access to independent financial, legal and operational advisers as required.

The appointment of the Responsible Officer should be reviewed on an 'as needed' or at minimum annual basis as part of the regular review of these procedures with consideration of resources and support made available to the Responsible Officer/s to ensure he/she/they have the means to discharge his/her/their responsibility under these procedures to a high standard.

Adequate resources are necessary to implement and maintain an effective whistleblower protection programme on an ongoing basis.

8. Current Responsible Officer at HSBC Continental Europe, Greece:

Constantina Tyrovoli , Chief Compliance Officer

Address: 109-111 Messoghion Ave. Athens Greece 115 26

Telephone: 00302106961104 (Monday to Friday 10:00 - 16:00)

E-mail: hsbc-confidential-greece@hsbc.com

Delegated Responsible Officer at HSBC Continental Europe, Greece:

Christina Krikelaidou, Compliance Manager

Address: 109-111 Messoghion Ave. Athens Greece 115 26

Telephone: 00302106961104 (Monday to Friday 10:00 - 16:00)

E-mail: hsbc-confidential-greece@hsbc.com

9. The Responsible Officer has the following responsibilities: a) provides appropriate information about the possibility of submitting a report within the organization and shares the relevant information in a visible place of the organization, b) receives reports about violations that fall within the scope of this law, c) confirms the receipt of the report to the reporting party via the HSBC Global Whistleblowing Team within a period of seven (7) working days from the day of receipt, d) takes the necessary actions via the HSBC Global Whistleblowing Team , in order for the report to be taken up by the competent bodies of the organization or the competent bodies as the case may be, or terminate the procedure, by archiving the report, if it is incomprehensible or is submitted abusively or does not contain incidents which establish a violation of EU law or there are no serious indications of such a violation, and the notification of the relevant decision to the petitioner who, if he considers that it was not dealt with effectively, may resubmit it to the National Transparency Authority (Εθνική Αρχή Διαφάνειας), which, as external channel, exercises the powers of article 12 of the Law, e) ensures via the HSBC Global Whistleblowing Team the protection of the confidentiality of the identity of the reporting person and any third party named in the petition, preventing access to it by unauthorized persons, f) monitors the petitions via the HSBC Global Whistleblowing Team and keeps in touch with the reporting person and, if necessary, request further information from him, g) provides information via the HSBC Global Whistleblowing Team to the reporting person about the actions taken within a reasonable period of time, which does not exceed three (3) months from the acknowledgment of receipt, or if no acknowledgment has been sent to the reporting person, the three (3) months from the end of seven (7) working days from the submission of the report, h) provides clear and easily accessible information on the procedures by which reports can be submitted to the National Transparency Authority (Εθνική Αρχή

Διαφάνειας) and, as the case may be, to public bodies or institutions and other bodies or organizations of the European Union, and i) plans and coordinates training activities related to ethics and integrity, participates in the formulation of internal policies to strengthen integrity and transparency to the Bank.

9. Anonymous Reporting / Reporting by Name and Confidentiality

Reporting Persons have the right to submit Reports at their discretion either anonymously or by their name. In the process of submission, the relevant call recordings will however be collected and processed by the Designated Officer.

Call recordings and data produced in the conduct of the Whistleblowing procedure will be treated as personal data of the Reporting Persons.

As a result, HSBC does not guarantee the anonymous nature of Reporting to persons falling under the scope of this policy.

Personal data and any information that leads, directly or indirectly, to the identification of Reporting Persons shall not be disclosed to any party other than the Designated Person and the staff authorized by the latter to receive or monitor Reports.

The identity of Reporting Persons and any other information about the handling of Reports may be disclosed only in the cases required by Union or Greek law, in the context of investigations by competent authorities or in the context of judicial proceedings, and if this is necessary for serving the purpose of protecting or ensuring the defense of Reporting Persons.

Disclosures about the identity of Reporting Persons and any other information about the handling of Reports are made after the Reporting Person has been informed in writing about the reasons for the disclosure, unless such notice undermines Investigations or judicial proceedings. After being informed, Reporting Persons shall be entitled to submit written observations to the Designated Person. Only in the event that such observations are not adequately justified, the disclosure of the identity and other confidential information of the Reporting Person will take place.

Confidentiality: The Bank ensures the confidentiality of the personal data and any information that may lead to the identification of the whistleblower, the person concerned, and any third party mentioned in such report, during both report follow-ups and communication with the competent authorities. Generally, any processing activity in the context of the internal reporting channel, must be in compliance with General Data Protection Regulation (EU) 2016/679 (“GDPR”) and Law 4624/2019, which supplements the GDPR in the Greek legal framework. In this regard, the Law sets out certain exemptions regarding transparency obligations, responding to data subject requests and notifying breach incidents. Companies must maintain a record for each report; specific provisions regulate how reports made verbally (e.g., by telephone or physical meeting) can be recorded.

10. PERSONAL DATA ISSUES

The main Data Protection pillars that the legislation is supposed to protect concern:

a) Protection of Personal Data.

The identity and personal data of every Reporting Person, Person Concerned, Involved Persons and, generally, third persons referred to in the Report, such as witnesses or colleagues, are protected at all stages of the Whistleblowing Process.

The Designated Persons refrains from collecting personal data not directly related with or not necessary for the handling of Reports and, if collected, immediately erases them.

b) Transparency of Processing.

Notwithstanding any other provisions of this Policy, HSBC takes appropriate measures to timely provide by electronic means to data subjects any information relating to the processing in a concise, transparent, and easily accessible form, using clear and plain language.

c) Data Collected during Telephone Calls.

Where a recorded telephone line or another recorded voice messaging system is used for reporting, HSBC may record the relevant call in a durable and retrievable form, subject to the consent of the Reporting Person.

In case that the Reporting Person does not consent, the Responsible Officer or the Navex representative shall write accurate minutes of the relevant conversation and offer the Reporting Person the opportunity to check, rectify and agree by signing them.

d) Data Collected during Physical Meetings.

Where the Reporting Person requests a physical meeting with the Designated Person, the latter shall write down accurate minutes of the relevant conversation in a durable and retrievable form, subject to the consent of the Reporting Person. The Designated person shall offer the Reporting Person the opportunity to check, rectify and agree by signing them.

e) Irrelevant or Accidentally Collected Data.

Personal data which are manifestly not relevant for the handling of a specific Report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

f) Data Subject Rights.

The Bank may reject requests of Persons Concerned and Involved Persons to exercise their rights under articles 15-22 GDPR for the time period necessary for the prevention or obstruction of Investigations or Follow-Up Actions or attempts for the identification of Reporting Persons or for the protection of Reporting Persons from retaliation.

In the examination of requests, the Bank takes the following steps:

- Evaluation of the fulfillment of the conditions of articles 15-22 GDPR for the exercise of the rights by data subjects;
- Evaluation of the fulfillment of conditions for the application of the restrictions to data subject rights of Law 4990/2022;
- Assessment of the necessity and proportionality of the restrictions vis-à-vis the rights of data subjects.
- Documentation of the reasons for satisfying or rejecting the requests;
- Taking additional measures, if necessary, to protect the rights of applicants.

In case of rejection, the Bank provides applicants with the reasons thereof and informs them about their right to submit a relevant complaint before the Greek Data Protection Authority.

g) Privacy by Design and by Default.

HSBC implements appropriate technical and organizational measures for ensuring that data protection principles are incorporated by design throughout the Whistleblowing Process and that, by default, only personal data which are necessary for each specific purpose of the processing are processed, including the following:

- Abstention from any processing of personal data for purposes other than those explicitly specified in article 1 of this Notice.
- Access to personal data related to the Whistleblowing Process on a need-to-know basis.
- Appropriate organizational and technical measures of data minimization and storage limitation throughout the life cycle of personal data.
- Implementation of corporate process for addressing data subject rights.
- Monitoring of the Whistleblowing Process by the Data Protection Officer.
- Security of Data.

HSBC implements appropriate technical and organizational measures to ensure a level of security for personal data related to the Whistleblowing Process, which is appropriate to the risk vis-à-vis data subjects' rights, including the following:

- The Designated person complies with strict conditions of confidentiality at all the stages of the Process.
- The corporate Register of Whistleblowing Reports and Investigations is separately stored and retained only in electronic encrypted form.
- Appropriate corporate policies and technical measures are in place to ensure, monitor and assess the ongoing confidentiality, integrity, availability and resilience of processing systems involved.
- Recipients of Data.
- HSBC has already assigned the operation of the reporting channel to Navex and may further assign parts of the Whistleblowing process, such as the receipt and processing of Reports and, generally, the processing on the behalf of HSBC of any data related to the Whistleblowing Process to third parties, which offer appropriate guarantees of respect for independence, confidentiality, data protection and secrecy (e.g. external reporting platform providers, external counsels, auditors).
- The transfer of information related to Reports and Investigations to competent supervisory and law enforcement authorities may take place for the establishment, exercise or defence of legal claims in the context of judicial proceedings.

i) Data retention periods.

Reports and any information and data generated in the course of Whistleblowing Processes shall be stored for a period of five (5) years from the closure of the process, unless further retention is necessary and proportionate for the purposes of processing specified in article 1 of this Notice or for the needs of ongoing judicial proceedings related to the subject matter of a specific Report.

j) Data Subjects' Rights.

The exercise of data subjects' rights shall be restricted to the extent and as long as necessary to prevent and address attempts to hinder reporting or to impede, frustrate or slow down Follow-Up, in particular investigations, or attempts to find out the identity of Reporting Persons.

11. Protection of whistleblowers. The Law prohibits any form of retaliation against whistleblowers, including threats of retaliation and attempts of retaliation including, indicatively, in the form of suspension, dismissal, demotion or withholding of promotion, change of location of place of work, reduction in wages, change in working hours, withholding of training, discrimination, disadvantageous or unfair treatment, failure to renew, or early termination of, a temporary employment contract, etc. Moreover, whistleblowers who do suffer retaliation may be entitled to compensation. Also, any termination of employment in the form of retaliation is invalid. Last but not least, whistleblowers are entitled to free legal advice and representation from lawyers included a relevant legal aid catalogue.

More specifically Law 4990/2022 (Part Z, Article 17) provides for the necessary measures to prohibit any form of retaliation against reporting persons, including threats of retaliation and attempts of retaliation including in particular in the form of: (a) suspension, lay-off, dismissal or equivalent measures; (b) demotion or withholding of promotion; (c) transfer of duties, change of location of place of work, reduction in wages, change in working hours; (d) withholding of training; (e) a negative performance assessment or employment reference; (f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty; (g) coercion, intimidation, harassment or ostracism; (h) discrimination, disadvantageous or unfair treatment; (i) failure to convert a temporary employment contract into a permanent one; (j) failure to renew, or early termination of, a temporary employment contract; (k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income; (l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry; (m) early termination or cancellation of a contract for goods or services; (n) cancellation of a licence or permit; (o) psychiatric or medical referrals. n) refusal or deprivation of providing reasonable accommodations to persons with disabilities. According to Law 4990/2022 (Article 22) Any term or agreement that waives or limits any rights and remedies provided herein, including a clause or agreement of arbitration, is void as to this limitation result.

Moreover, whistleblowers who do suffer retaliation may be entitled to compensation.

12. Penalties: The Law provides for both criminal sanctions and monetary fines for persons who (a) obstruct or attempt to obstruct reporting, (b) retaliate or bring vexatious proceedings against reporting persons and (c) infringe the obligation of confidentiality of the identity of reporting persons. On the other hand, Law provides for penalties applicable in respect of reporting persons where it is established that they knowingly reported or publicly disclosed false information.

13. External Reporting: the oral or written or via an electronic platform communication of information on breaches towards the National Transparency Authority (Εθνική Αρχή Διαφάνειας) in its capacity as the competent authority for the acceptance/receipt, management and monitoring of reports submitted towards the latter directly.

Procedure for External Reporting: The external report is submitted in writing or orally – via telephone or other systems of oral messaging, and via a personal meeting – or via an electronic platform, accessible to persons with disabilities, that is operating on the website of the public or private entity.

14. Public disclosure: the making of 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 (Εθνική Αρχή Διαφάνειας), 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 (Εθνική Αρχή Διαφάνειας), 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.

III. PRIVACY NOTICE GREECE - NOTICE ON THE OPERATION OF THE INTERNAL REPORTING CHANNEL & THE RELEVANT PROCESSING OF PERSONAL DATA

HSBC Continental Europe is legally established in Greece by virtue of a branch registered in the General Commercial Registry (GEMI) (“HSBC”), with headquarters in Athens, 109-111 Mesogeion Avenue, hereinafter referred to as the "Company") has established and put into operation an internal reporting channel ("Channel") under the Law. 4990/2022 "Protection of persons reporting breaches of EU law" (Government Gazette 210/A/11-11-2022).

With this form, the Company provides the following information: (a) in its capacity as an obligated person under Law 4990/2022, informs the persons who have the right to submit reports through the Channel about the operation of the Channel, the procedures for following up on reports and their rights, and (b) in its capacity as data controller, informs data subjects about the processing of their personal data during the operation of the Channel and the management of reports.

A. Operation of the Internal Reporting Channel in accordance with Law 4990/2022

Internal reports to the Company are submitted to the Channel, provided by NAVEX GLOBAL The Ethics and Compliance Experts ("Navex") on behalf of the Company and via Responsible Officer local recorded line.

Reporting Persons may submit reports both by name and anonymously.

The internal report is submitted in writing (e mail, letter, Executive Referral). Alternatively, the report may be submitted orally through an electronic platform which operates on the website and the intranet of HSBC (HSBC Confidential). The verbal report can be submitted via telephone either via local recorded line 0030 210 6961104 or via NAVEX call center (HSBC Confidential) as above as well as through a personal meeting with the Person in Charge of Receipt and Follow-up of Reports within a reasonable time, at the request of the reporting person.

Bank’s Responsible Officer is responsible for receiving any reports via the local recorded line and re direct to HSBC Global Whistleblowing Team (HSBC Confidential) in order to take all necessary steps when conducting any required investigations. This includes performing a

preliminary review of reports received from reporting persons in accordance with the Law and assigning the report for investigation. Personal data and any kind of information leading, directly or indirectly, to the identification of the reporting person, are kept strictly confidential and are not disclosed to any third party other than the Designated Person and the authorized staff members responsible for receiving, or following up, reports.

As an exception, the identity of the reporting person and any other information may be disclosed only in the context of investigations by competent authorities or in the context of judicial proceedings, if provided by law and necessary to serve the purposes of Law 4990/2022 or to safeguard the defence rights of a reporting person. Such disclosure shall take place only after the reporting person has been informed in writing and is given the right to submit written objections to the Company.

The operation of the Channel as well as the receipt, monitoring, management and archiving of reports are further determined in detail by the specific terms of the Company's policy on Whistleblowing, as in force from time to time, which supplements the information in this form and is available at the following link: hsbc-confidential-greece@hsbc.com

Without prejudice to the law, reporting persons shall not be liable, inter alia, in relation to (a) obtaining information or accessing the information reported, provided that such acquisition or access does not in itself constitute a criminal offence, and (b) reports as such, if they have reasonable grounds to believe that the report was necessary to reveal a breach.

Any form of retaliation against reporting persons, their relatives or colleagues, intermediaries and businesses of their interests or undertakings in which they are employed, including threats and acts of retaliation, shall be prohibited. In case of retaliation, these persons may appeal to the Designated Person and will be entitled to compensation for any damages inflicted.

Each reporting person has the right to submit an external report to the National Transparency Authority ("NTA") in the following ways: (a) electronically by sending an e-mail to kataggelies@aead.gr or by filling out a digital form on https://aead.gr/submit-complaint/ website, (b) by post, by sending a written letter to the following address: National Transparency Authority, L. Lenorman 195 and Amfiaraou, 10442, Athens, as well as (c) in person at the above headquarters of the NTA.

Upon request, the Designated Person shall provide Reporting Persons with appropriate information on the right to report, as well as information on the procedures under which an external report can be submitted to the NTA and, where appropriate, public bodies or institutions, bodies, offices or agencies of the European Union.

Any matter relating to the process of submitting, monitoring, managing and archiving reports, the protection of Reporting Persons and, more generally, the operation of the Channel and the submission of external reports to the NTA can be addressed to the Designated Person, by sending a relevant request to the following e-mail account: hsbc-confidential-greece@hsbc.com

B. Processing of Personal Data during the Operation of the Internal Reporting Channel

During the operation of the Channel, the Company may process the data of the following categories of data subjects, as defined in Law 4990/2022: (a) reporting persons, (b) persons concerned, (c) facilitators, and (d) third persons who may be identified in reports or follow-up actions.

The data processed are data included in reports, as well as data processed during the submission, monitoring, management and archiving of reports, data about the actions taken to protect reporting persons and, more generally, the operation of the Channel and the implementation of the Company's Whistleblowing policy and which concern or are related to violations of rules of law falling within the scope of Law 4990/2022. Data sources are reporting persons, persons concerned, facilitators as well as third parties from whom data are collected in carrying out follow-up actions.

The purposes of processing are the following: (a) the fulfillment of the obligation to establish and operate the Channel, (b) the submission, monitoring, handling and archiving of reports, (c) the execution of follow-up actions and, in general, the taking of the necessary measures for the follow-up of submitted reports; (d) the protection of reporting persons, in particular against retaliation; (e) disciplinary measures and/or judicial proceedings against persons concerned who commit infringements; (f) the provision of information on alleged criminal offences to competent law enforcement and judicial authorities; (g) the security and confidentiality of the whistleblowing process and the data processed in relation to it; (h) the establishment, exercise or support of legal claims of the Company or third parties; and (i) the improvement of the organization and administration of the Company.

The legal basis for the processing is, on the one hand, the compliance of the Company with its legal obligations, as provided for in Law 4990/2022, as well as the pursuit of the Company's legitimate interests for the proper functioning of its business and the prevention, suppression, criminal prosecution and compensation for violations of the law (Article 6 § 1 (c)) and (f) GDPR) and, on the other hand, the processing for the establishment, exercise or support of legal claims of the Company or third parties as well as for reasons of substantial public interest based on Law 4990/2022 (article 9 § 2 (f) and (g) GDPR).

Our Company will retain your personal data for a period of five (20) years from the completion of the follow-up of the respective report or the taking of measures to protect the reporting persons or the taking of disciplinary measures and/or legal actions against reporting persons or third parties. Our Company may retain your personal data after the expiration of the aforementioned period in the following limited cases: (a) if this is necessary and for as long as it is required for the fulfillment of the purposes of processing, or (b) if there is a legal obligation of ours by a relevant provision of law, or (c) to defend our rights and legitimate interests before any competent Court and any other public authority within the foregoing limitation period.

The following categories of processors on behalf of the Company have access to personal data: (a) Navex in the context of providing the Channel, (b) IT service providers in the context

of supporting and hosting the Company's information systems, and (c) professional advice providers in support of follow-up actions. The Company may transmit personal data to lawyers and law firms for the provision of legal services for the purpose of establishing, exercising or supporting legal claims of the Company. The Company may transfer personal data to its parent company as well as to affiliated companies of the HSBC Group for the purpose of organizing and managing reports at Group level, to subcontractors, agents and service providers. In any case, transfers of relevant information as well as investigations to the competent authorities or law enforcement authorities may take place in the context of the performance of legal obligations of the Company or the exercise or support of its legal claims.

In the context of whistleblowing, we may transfer your data to third countries outside the European Economic Area (EEA). Where this is the case, we ensure before the transfer that appropriate safeguards are put in place to require that your personal data will remain protected in accordance with this data protection notice and that the recipient will guarantee an adequate level of protection of your data. This may include that the recipient implements Standard Contractual Clauses for transfers of personal data, which require the recipient to protect personal data in accordance with EU data protection law. For information on the appropriate safeguards we have in place, you can contact us at the details provided above.

Without prejudice to the law, you may exercise, where applicable, the rights provided for in Articles 15-22 of the GDPR for access, rectification, erasure, restriction of processing, portability or objection to the processing of your personal data or objection to automated decision-making, including profiling, by sending a relevant request to the email account: hsbc-confidential-greece@hsbc.com.

The Company may justifiably reject the relevant requests of the parties involved, for the period deemed critical to obstruct investigations or actions towards the completion of the procedure or the protection of reporting persons.

In addition, you may submit a complaint to the Personal Data Protection Authority (L. Kifisias 1-3, P.C. 115 23, Athens, telephone: 210 6475600, https://www.dpa.gr/el/syndesi/prosvasi).