

## **PERSONAL DATA PROCESSING NOTIFICATION**

### **in the context of the Union Law Breaches Reporting System**

#### **1. Introduction**

This Personal Data Processing Notification applies to all natural persons who submit, either by name or anonymously, a report within the framework of the Union law breaches reporting system that has been implemented (the “Report”) concerning breaches that have been committed or are highly likely to be committed.

**THIS NOTIFICATION SUPPLEMENTS ANY OTHER NOTIFICATION THAT WE MAY HAVE PROVIDED TO YOU AND CONSTITUTES AN INTEGRAL PART OF THE UNION LAW BREACHES REPORTING POLICY.**

In this Notification, the terms “we” / “us” and/or “HAU” refer to the Hellenic American Union (22 Massalias Street, Athens, Attica, Postal Code 10680, Tel.: 2103680000, Email: [privacy@hau.gr](mailto:privacy@hau.gr)), which is also the controller of the relevant data.

HAU does not provide information regarding the processing of personal data to the Reported Person and to Witnesses, as defined in Section 2 below, for as long as required and where deemed necessary for the purpose of preventing and addressing attempts to obstruct reporting, hinder, frustrate or delay follow-up actions, particularly with regard to investigations, or attempts to identify Reporting Persons, as defined in Section 2 below, as well as for the purpose of protecting them against retaliation.

#### **2. Types of Personal Data and Categories of Natural Persons**

During the reporting procedure, HAU, acting in its capacity as data controller, may collect personal data relating to the following persons (collectively, the “data subjects” and/or “you”):

- Natural persons who submit a Report by providing information concerning breaches falling within the scope hereof (the “Reporting Person”);
- Natural or legal persons named in the Report as persons to whom the breach falling within the scope hereof is attributed (the “Reported Person”);
- Third-party natural persons who are not named in the Report as Reported Persons but are merely referred to therein and/or contribute additional information and/or documentary evidence regarding the reported incident (the “Witnesses”).

The types of personal data that HAU may collect during the aforementioned procedure include:

(a) your personal information (such as information collected through the system for the purpose of submitting the Report, including full name, date of birth, telephone number (landline/mobile) and email address);

(b) employment-related data (such as job position, business unit, duties and annual performance evaluations); and

(c) any information contained in the Report relating to the reported breach incident, such as the location and time of the incident, additional information or available evidence, the manner in which you are connected to the incident and to the person against whom the Report is submitted, any other persons involved in the incident whom you suspect, and information that may relate to the Reporting Person himself/herself or to any other natural person referred to above, as well as the content of the Report (e.g.

information relating to accounting matters, internal accounting controls or auditing procedures, offences in the banking or financial sector, and bribery cases to which the reported incidents relate).

The disclosure of the data referred to in points (a) to (c) above constitutes a prerequisite for the initiation of an investigation following the submission of the Report, in order to determine whether the reported act or event is substantiated.

When using the system, you are strongly advised to ensure that any personal data included in the Report relating to yourself or other persons are strictly limited to what is necessary for the purpose of the Report and strictly and objectively necessary for us to verify the reported acts.

### **3. Source of Personal Data**

HAU collects personal data directly from the above-mentioned data subjects.

### **4. Legal Basis for the Processing of Personal Data**

The legal basis for the collection, processing and use of personal data within the framework of the breach reporting procedure is set out in Article 6(1)(c) and (f) of the GDPR. This means that we process your data either in order to comply with a legal obligation to which we are subject or for the purposes of the legitimate interests pursued by HAU, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subjects.

### **5. Purposes of the Processing of Personal Data**

During the procedure carried out through the reporting system, HAU collects, uses and generally processes the personal data of data subjects, as applicable, for the following purposes:

- (1) to manage the internal breach reporting system and ensure the security of the processing operations carried out through the system;
- (2) to ensure compliance with internal policies and limit incidents of misconduct;
- (3) to ensure the implementation of appropriate corporate governance principles in day-to-day operations;
- (4) to comply with any applicable laws and regulations relating to breach reporting (e.g. prior notification or reporting requirements, as applicable, to national authorities);
- (5) to conduct investigative procedures regarding the relevance and substantiation of the reported facts;
- (6) for use in connection with any legal proceedings or regulatory actions (including future proceedings and actions) and for obtaining legal advice or establishing, exercising or defending legal rights; and
- (7) to impose sanctions in the event of misuse of the reporting system by the responsible person.

### **6. Recipients of Personal Data**

Personal data shall be processed exclusively by competent and duly authorised employees and bodies of HAU responsible for the management of Reports and contractually bound by confidentiality obligations, as well as by the Reports Receiving and Monitoring Officer (“RRMO”).

Such data may also be disclosed to affiliated service providers with whom HAU has entered into contractual arrangements and which process data on HAU's behalf (e.g. providers of reporting system management services or services relating to the conduct of necessary investigations, etc.), within the scope of their responsibilities and subject to obligations of confidentiality, secrecy and compliance with personal data protection legislation. Furthermore, personal data may be disclosed to or processed by selected third-party professionals, such as external lawyers or consultants.

Finally, HAU may disclose personal data to third parties where required by law (e.g. obligations of prior notification to competent authorities), in the context of or in connection with legal proceedings in which it is involved, for the support, exercise or defence of its rights, to law enforcement authorities that have submitted a valid disclosure request, or where it considers such disclosure necessary in connection with any investigation relating to suspected or actual unlawful activity.

Where the data contained in Reports may be used as evidence in administrative, civil or criminal investigations and proceedings, such data shall also be disclosed to the competent supervisory, investigative and prosecutorial authorities.

HAU guarantees the confidentiality of every Report and of the information contained therein, as well as the anonymity of the Reporting Person, even where the Report is subsequently proven to be incorrect or unfounded. In particular:

- Personal data and any type of information that directly or indirectly leads to the identification of the Reporting Person shall not be disclosed to any person other than the authorised members of staff responsible for receiving or following up Reports, unless the Reporting Person has expressly consented thereto.
- Any other disclosure of data shall take place only where the Reporting Person has provided his/her explicit consent or where disclosure is required under applicable Union or national law and in accordance with the relevant applicable conditions.
- By way of exception to the above, the identity of the Reporting Person and any other information may be disclosed only in cases where this is required by Union or national law, in the context of administrative, civil or criminal investigations conducted by competent public authorities or in the context of judicial proceedings, and provided that such disclosure is necessary for the purposes of Union or national law or for safeguarding the rights of defence of the Reported Person.

The above provisions regarding the protection of the identity of Reporting Persons shall also apply to the protection of the identity of Reported Persons.

Reports shall be stored confidentially and retrieved where required by Union or national law and, in any event, until the completion of any investigation or judicial proceedings initiated as a consequence of the Report.

## **7. Cross-Border Transfers**

The personal data contained in Reports shall not be transferred to countries outside the European Economic Area.

## **8. Your Rights in Relation to Personal Data**

Under certain circumstances and in accordance with the applicable legislation, you have the right to:

- Request access to your personal data (commonly known as the “data subject access right”). This enables you to receive a copy of the personal data we hold about you.
- Request the rectification of the personal data we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request the erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no valid reason for us to continue processing it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
- Object to the processing of your personal data where we rely on our legitimate interests (or those of a third party) and there is something about your particular situation which makes you wish to object to processing on that ground.
- Request the restriction of the processing of your personal data. This enables you to ask us to suspend the processing of your personal data, for example if you want us to establish its accuracy or the legal basis for processing it.
- Where we process personal data by automated means:
  - where we process your personal data on the basis of your consent; or
  - where such processing is necessary for entering into or performing obligations undertaken under a contract concluded with you,
- request the transfer of your personal data to another party (also known as the “right to data portability”).
- Withdraw your consent at any time where we process your personal data on the basis of your consent. If you do not provide or subsequently withdraw your consent, we may be unable to provide our services to you. It is noted that the withdrawal of your consent shall not affect the lawfulness of processing based on consent before its withdrawal.
- Request, in certain circumstances, not to be subject to decisions based solely on automated processing, including profiling.

Certain of the above rights are not absolute under the applicable legislation (for example, there may in some cases be overriding legitimate grounds requiring the continuation of processing). Furthermore, HAU may refuse to satisfy the above rights where they are exercised by Reported Persons or Witnesses, or where such rights arise in connection with follow-up measures relating to a Report.

Should you wish to receive further information regarding the processing of your personal data or to exercise any of the above rights, you must send an email to HAU exclusively at: [privacy@hau.gr](mailto:privacy@hau.gr), or send a letter to the postal address indicated above.

Finally, you have the right to lodge a complaint with the competent supervisory authority in the country where you work or reside, or where you believe an issue concerning your personal data has arisen (for Greece: [www.dpa.gr](http://www.dpa.gr)).

## **9. Retention of Personal Data**

The retention period for the above data shall be the period required or permitted by the applicable legislation and regulatory framework in force from time to time, taking into account the applicable statutory limitation periods, which may extend up to twenty (20) years.

In particular:

(a) where a Report is assessed as unfounded, the retention period for the relevant data shall be two (2) months from the dismissal of the Report;

(b) where legal proceedings or disciplinary measures are initiated against the Reported Person or the Reporting Person, the personal data shall be retained until the completion of such proceedings and the expiry of the applicable period for exercising legal remedies, in accordance with the applicable legislation;

(c) where a Report reveals substantiated findings against an executive, officer or employee of HAU, the personal data shall be retained for the duration of his/her employment or relationship with HAU and shall be deleted twenty (20) years following the termination of such relationship, regardless of the manner of termination; and

(d) where a Report reveals substantiated findings against an external associate or supplier of HAU, the personal data shall be retained throughout the duration of the relevant business relationship and shall be deleted five (5) years after the termination thereof, regardless of the manner of termination.

## **10. How to Contact Us**

If you wish to exercise any of your rights in relation to your personal data or obtain additional information regarding the retention periods applicable to your personal data, please contact HAU at [privacy@hau.gr](mailto:privacy@hau.gr).

## **11. Updates**

HAU may update this Notification periodically due to changes in legislation, regulations, internal procedures or systems, and will inform you of any material changes through appropriate communication channels. All changes shall become effective as of the date of publication unless otherwise specified.