



Conduct Watch Platform | Privacy Notice

Last revised: February 2024

“Deloitte Business Solutions Societe Anonyme of Business Consultants” (hereinafter “Deloitte”, “we”, “us” or the “Firm”), hereby informs you, in its capacity as a data processor, regarding the processing of your personal data, in the context of providing independent whistleblowing services (hereinafter the “Services”) to its clients, who act as data controllers, using the Whistleblowing Conduct Watch Platform (hereinafter “Conduct Watch” or the “Platform”).

Conduct Watch is used by the data controller (your employer, client, business partner or other business relationship) to manage whistleblowing cases under the provisions of Greek Law 4990/2022, as applicable, and Directive (EU) 2019/1937 of the European Parliament and European Council on the protection of persons who report breaches of Union Law.

This privacy notice explains what information is collected about you, how that information is used and to whom that information is disclosed in the course of providing the afore mentioned Services to the data controller. It also sets out your rights in relation to your personal data and who you can contact for more information or queries.

Useful Definitions:

‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

‘Controller’ means the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

‘Third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to

process personal data;

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'Special categories of personal data' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

Purposes regarding the processing of your personal data:

When we process personal information through Conduct Watch Platform in the context of providing whistleblowing services to our clients (data controllers), the specified purpose(s) of the processing of your personal data are determined by the data controller and the processing is carried out by Deloitte, on behalf of the data controller, only according to the documented instructions received by the latter.

Categories of personal data we process & sources of personal data:

The personal data typically processed during the provision of the abovementioned Services, may be categorized as follows:

- Personal data provided in the submitted report(s), including any follow-up communications that may take place during the whistleblowing process, for instance, data that may be included in the description of the incident, the names and other identification details of the person to whom the breach is attributed or with whom that person is associated, names and other identification details of witnesses or any other involved persons, if any;
- Personal data included in the supporting material/documentation of the internal report, if any;
- In case of non-anonymous reports, identification data of the reporting person (yourself) ;
- In case the voice messaging system reporting feature is activated, voice data;
- Digital footprint data (IP address, browser type & language and access time to the application). It is highlighted though that these data will be used solely for technically establishing a secure communication channel and will not be processed in the Platform, hence the identification (directly or indirectly) of the reporting person will not be possible;
- Personal data required to authenticate and authorize users into Conduct Watch platform, as well as audit logs (applicable only to data controller's authorized persons to access the Platform, e.g., admins).

Kindly note that due to the nature of the Services (i.e., the nature of some reports that may be submitted in the Platform), special categories of personal data may be processed as well.

Sources of the personal data collected are the reporting person (yourself) and potentially any other person that may be involved in the course of an investigation (if any).

In addition, when you use the Platform, strictly necessary cookies and similar technologies to operate the application are used. Additional information on how cookies are used can be found in the [Cookies Notice](#).

Legal basis for the processing:

The legal basis for the processing of your personal data is determined by the data controller. Should you have any

questions about the legal basis for the processing of your personal data, please directly contact the data controller. The basis for processing of your personal data may include compliance with the data controller's legal obligation arising out of Law 4990/2022, as applicable and in particular the obligation to operate internal reporting channels and to take the necessary measures for the follow-up on the reports. Furthermore, according to law 4990/2022, the recording via the voice messaging system, when used for reporting, is subject to the consent of the reporting person (you).

It should be noted that Deloitte, as the data processor, will carry out the processing strictly as per the instructions of the data controller, whilst ensuring that the processing will be reduced to the minimum and that every operation made will be done with the strictly necessary means for the purposes determined by the data controller, adopting any measure to mitigate or reduce the extent and impact of the data processing.

Recipients of your personal data:

Your personal data are disclosed, through the Platform, to the authorised personnel of the data controller and/or other appointed persons of the data controller.

In addition, when it is necessary to fulfill one or more of the purposes determined by the data controller in the context of the provided Services, recipients of your personal data are entities that provide services to us and/or the Deloitte Network. Namely the following entities may have access to your personal data:

- a. Deloitte Consultanță SRL (Deloitte Romania): authorized personnel may have access to the Platform only for administrative and bug fixing purposes and thus may have access to personal data strictly for the provision of technical support services to the users of the Platform.
- b. Amazon Web Services (AWS) providing hosting services (IaaS) through data centers in Frankfurt, Germany.

In relation to the abovementioned service providers, it is noted that your personal data will not be transferred to countries outside the European Economic Area.

Kindly note that, we may be requested to further disclose your personal data if required to do so by law, a regulator or during legal proceedings.

Protection of your personal information:

We have in place reasonable commercial standards of technology and operational security to protect all your personal information from misuse and unauthorized access, loss, disclosure, alteration or destruction. Only authorized personnel, who have been made appropriately aware of our privacy obligations, are provided access to personal information.

How long we keep your information:

The retention period of your personal data is determined by the data controller unless further storage is required by applicable law. Thus, should you have any questions about how long your personal information is retained, please contact the data controller directly.

Your rights:

According to articles 12-22 of the General Data Protection Regulation (GDPR), you have the following rights:

- (a) The right to obtain **transparent information as to whether or not personal data concerning you are being processed** and, where that is the case, access to the personal data and to further information provided for in art.15 GDPR.
- (b) The right to request the **rectification of incorrect, inaccurate or incomplete personal data**. Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- (c) The right to request the **erasure of personal data** concerning you, in cases provided by the applicable legislation.
- (d) The right to request **restriction of processing of your personal data**, in cases provided by the applicable legislation.
- (e) The right to **receive without any cost accrued your personal data in a structured, commonly used and machine-readable format**, as well as the right to transmit those data to another controller, provided that it is technically feasible. This right concerns the data that you have provided and their processing is carried out by automated means based on your consent or in performance/execution of a relative contract.
- (f) The **right to object**, on grounds relating to your particular situation, at any time to processing of personal data concerning you, in cases provided by the applicable legislation.
- (g) The right **not to be subject to a decision based solely on automated processing**, including profiling, which produces legal effects concerning you or similarly significantly affects you.
- (h) The right to **withdraw your consent** at any time (in cases where consent is the legal basis of the processing). The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Should you wish to exercise any of your abovementioned rights in relation to the personal data that Deloitte may have processed on behalf of the data controller, please contact the data controller directly or Deloitte by sending an email to the following address: DataPrivacyOfficer@deloitte.gr. The Firm would like to inform you that, even though we are committed to respecting your rights, we might not be able to respond directly to your requests and/ or inquiries. However, we will promptly forward any question, complaint and/or request to the data controller, as soon as possible and in any case within the contractually agreed upon timeframe, and we will make every possible effort to support the data controller in satisfying your rights, unless prohibited by law.

Notwithstanding the foregoing, if you have any questions or complaints about the way we handle your personal information, you may contact the Firm's DPO by sending an email to the following address: DataPrivacyOfficer@deloitte.gr. We will make every possible effort to resolve any issue, either independently, where permitted under our contract with the data controller, or by referring the request to the data controller.

You always have the right to file a complaint before the competent supervisory authority, which in Greece is the Hellenic Data Protection Authority (HDP), by following the instructions found on the HDP's [website](#).