



INFORMATION ON THE PROCESSING OF PERSONAL DATA
PURSUANT TO ART. 13-14 EU REG. 2016/679

Data Subjects: whistleblowers, persons to whom the breach is attributed and any other third parties involved in the management of reports governed by the Whistleblowing Policy document.

Sonders and Beach World S.r.l. with head office in Milan, Via San Gregorio, 27, as the Data Controller, pursuant to and for the purposes of Regulation (EU) 2016/679 (hereinafter "GDPR"), hereby informs you that the personal data of whistleblowers, persons to whom the breach is attributed and third parties who are connected with the breach (hereinafter "Data Subjects") will be processed for the management of whistleblowing reports, governed by the Whistleblowing Policy document (hereinafter "Policy") approved by the Board of Directors of Sonders and Beach World S.r.l.

Contact information of the Data Controller: E-mail: amministrazione@sondersandbeach.com

Contact office: Via San Gregorio, 27, 20124 Milano (MI).

Data Protection Officer (DPO)

The Data Controller has appointed a Data Protection Officer (DPO) who is available for any information and requests at the following e-mail address: amministrazione@sondersandbeach.com

Personal data processed. Special categories of personal data and data relating to criminal convictions and offences.

The following data may be processed: common data, data revealing racial or ethnic origin, political opinions, religious and/or philosophical beliefs, trade union membership, as well as genetic data, biometric data, data concerning a person's health or sexual life or sexual orientation and data relating to offences and criminal convictions.

Source of personal data and categories of data collected c/o third parties.

The Data Controller collects data through reports. The data of Data Subjects, contained within the report, is provided directly by the whistleblower. Whistleblowers may be employees and/or collaborators, directors, consultants and, in general, any person persons falling within the subjective scope of Legislative Decree 24/2023. Reports may be nominal or anonymous. In order to preserve the purposes of investigation, in the cases provided for by law, the person to whom the breach is attributed, pursuant to Article 14(5)(d) of the GDPR, may not be immediately made aware of the processing of his/her data by the Data Controller, as long as there is a risk of undermining the possibility of effectively verifying the merits of the complaint or gathering the necessary evidence.

Purpose and legal basis of the processing.

The personal data of the Data Subjects is processed for the purposes related to the application of the aforementioned Policy, established for the management of reports of unlawful conduct pursuant to Legislative Decree no. 24/2023 implementing the Directive (EU) 2019/1937 of the European parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

The following conducts may be considered objects of reporting:

- breach of European regulatory provisions on the following areas: public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection and security of networks and information systems;
- act or omission affecting the financial interests of the European Union;
- act or omission relating to the internal market that jeopardise the free movement of goods, persons, services and capital;
- act or conduct that frustrate the object or purpose of the provisions of Union acts;
- breach of national legislation implementing European Union law.

The adoption of the Policy and the consequent processing of personal data therefore take place on the basis of a legal obligation to which the Data Controller is subject. The Policy guarantees the confidentiality of the reporter's identity, handling personal data separately from the content of the report made. Any combination can only be carried out in the exceptional cases indicated in the Policy in accordance with the applicable legal provisions (e.g. in order to exercise the right of defence of the person to whom the breach is attributed, with the prior consent of the person making the report; in cases where the criminal liability of the whistleblower is established, including by a first-degree judgement, for offences of slander or defamation; in cases of reports that prove to be unfounded, made with malice or serious misconduct). Special categories of personal data and data related to criminal convictions and offences will be processed for this purpose, pursuant to Article 9(2)(b) and Article 10 of the GDPR respectively. With regard to any processing of personal data after the closure of the whistleblowing analysis procedure, the legal basis is the legitimate interest of the Data Controller in the exercise

of its rights in all cases where this is necessary (e.g. reopening of judicial proceedings, claims for damages related to the whistleblowing), pursuant to Art. 6, para. 1(f) and Art. 9, para. 2(f) of the GDPR.

Nature of provision and consequences of refusal

The provision of the whistleblower's data is compulsory in "nominal reports". A refusal to provide the data in the "nominal report" makes it an "anonymous report". However, the whistleblowing manager may indirectly derive the identity of the whistleblower from the information reported. In any case, the identity of the whistleblower and any other information from which such identity may be inferred may be disclosed only with the previous express consent of the whistleblower and in case it is necessary for the defence of the persons to whom the breach is attributed, as part of a disciplinary procedure or where in internal and external whistleblowing managing procedures the disclosure of the identity of the whistleblower is also necessary for the defence of the person to whom the breach is attributed.

Modalities of processing

Your personal data may be processed in the following ways:

- processing by means of automated tools (through the Whistleblowing platform, for example, using electronic procedures and supports) with logics related to the above-mentioned purposes and, in any case, in such a way as to guarantee the security and confidentiality of the data.

Communication

Independent data controllers to whom the data may be transmitted are: judicial authorities, ANAC, external lawyers with mandate, and private investigation companies. In exceptional cases, where the report has given rise to disciplinary proceedings and is based solely on the whistleblower's report, the identity of the whistleblower may be disclosed to the person subject to the disciplinary proceedings, if this is absolutely essential to exercise his/her right to defence. In such cases, the report will only be usable for the purposes of the disciplinary proceedings if the whistleblower has consented to the disclosure of his/her identity.

Retention period

Data is retained for 5 years starting from the closure of the report or for a longer period where necessary for res judicata effect of a judgement or other judicial measure, if any.

Data Processors and persons acting under the authority of the Data Controller

The Data Processor, pursuant to Article 28 of the GDPR, is EQS Group S.r.l. which manages the whistleblowing platform and ensures the storage of personal data processed in the cloud. It should be noted that the aforementioned supplier provides the necessary infrastructure for the implementation of the reporting procedure but does not access the content uploaded on it.

For the purposes of managing reports, the Data Controller appointed external data processors such as: the company responsible for managing reports. **Sonders and Beach S.r.l.** provides the Data Processor with operating instructions to ensure the confidentiality and security of the processing of personal data, ensure

compliance with applicable legislation and the protection of Data Subjects. Any person acting under the authority of the Data Controller, may be employees and/or collaborators of the Data Controller, shall process data on instructions of the Data Controller pursuant to Articles 29 of the GDPR and 2-quaterdecies of Legislative Decree no. 196/2003.

Rights of the Data Subject

Data Subjects may ask the Data Controller for access to the data concerning them, for their rectification, integration or cancellation, as well as for the restriction of processing or any other right pursuant to Articles 15 to 22 of the GDPR, subject to the conditions which shall be highlighted in the request. This is true unless there are legitimate reasons for overriding the interests, rights and freedoms of the Data Subject, the establishment, exercise or defence of a right in court or other legal obligations to be fulfilled by the Data Controller or any other provision of the public authorities or the judicial authorities or the police bodies. Data Subjects also have the right to lodge a complaint with the Data Protection Authority in the event of unlawful or illegal processing of their data by the Data Controller. Pursuant to Article 2-undecies letter f) of Legislative Decree no. 196/2003, as updated by Legislative Decree no. 101/2018, and Legislative Decree no. 24/2023, the rights set out in Articles 15 to 22 of the GDPR may not be exercised if this may result in real and actual prejudice to the confidentiality of the employee who reports unlawful conduct of which he/she has become aware by reason of his/her working activity.