NOTICE ON THE OPERATION OF THE INTERNAL REPORTING CHANNEL &

THE RELEVANT PROCESSING OF PERSONAL DATA

The ORFIUM Group of Companies (“Group”) encourages a corporate speak up culture in its workplace and ensures that its employees feel safe sharing their concerns and report misconduct about potential violations of European Union legislation.

In this context, the Group has established and put into operation an internal reporting channel ("Channel") under Directive (EU) 2019/1937 (“Whistleblowing Directive”), as transposed into national law in the country of the registered seat of each of its subsidiaries.

With this notice, our Group provides the following information to reporting persons and data subjects:

a. in its capacity as an obligated person under the Whistleblowing Directive, the Group 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, the Group 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 applicable law

Internal reports to the Group under applicable law are submitted by electronic means to the Channel, accessible at the following link: https://www.orfium.com/whistleblowing-reporting/ . Alternatively, internal reports may be submitted orally through a personal meeting with the Person designated to handle the Receipt and Follow-up of Reports (“Designated Person”) within a reasonable time, at the request of the reporting person.

Reporting Persons may submit reports both by name and anonymously. In the case of reports by name, the Group pseudonymizes the personal data being processed.

The Designated Person is responsible for receiving any reports through the Channel and for taking all necessary steps when conducting any required follow-up actions. 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 authorised staff members responsible for receiving, or following up on, 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 applicable law 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 Group.

The operation of the Channel as well as the receipt, monitoring, management, follow-up and archiving of reports are further specified in detail by the specific terms of the Group's Whistleblowing Policy, as in force from time to time, which supplements the information in this form and is available at the following link: https://www.orfium.com/whistleblowing-policy/ ("Policy").

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 offense, 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 competent public authority of the country of his / her employer subsidiary.

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 competent national public authority 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 competent national public authority can be addressed to the Designated Person, by sending a relevant request to the following e-mail account: tellme@orfium.com .

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

During the operation of the Channel, the subsidiary of the Group acting as employer jointly with the parent company of the Group ("Joint Controllers" or "Group") may process the data of the following categories of data subjects, as defined in applicable law: (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 Group's Whistleblowing policy and which concern or are related to violations of rules of law falling within the scope of the Whistleblowing Directive. 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 offenses 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 Group or third parties; and (i) the improvement of the organization and administration of the Group.

The legal basis for the processing is, on the one hand, the compliance of the Group with its legal obligations, as provided for in the Whistleblowing Directive, as well as the pursuit of the Group'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 Group or third parties as well as for reasons of substantial public interest based on the Whistleblowing Directive (article 9 § 2 (f) and (g) GDPR).

Our Group will retain your personal data for a period of five (5) 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 Group 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 Group may acquire access and process the personal data: (a) whistleblowing platform service providers, in the case that the Group chooses to outsource the electronic platform of the Channel; (b) ICT service providers in the context of supporting and hosting the Group's information systems, including the Channel; and (c) professional consulting service providers in support of the management and follow-up of reports. The Group may transfer 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 Group. The Group may transfer personal data to its parent Group as well as to subsidiaries and affiliates of the Group for the purpose of organizing and managing reports at Group level, and / or to their subcontractors, agents and service providers acting as their data processors. Transfers of data to competent or law enforcement authorities may take place in the context of the performance of legal obligations of the Group 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). When this is the case, prior to the transfer we ensure that appropriate safeguards are put in place so that your personal data remains 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 below.

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, 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: dpo@orfium.com.

The Group may justifiably reject data subject requests according to the provisions of any legislation applicable, for the period necessary for the purposes of (i) preventing and countering attempts to prevent reporting; and / or (ii) obstructing, thwarting or delaying follow-up actions, especially in relation to investigations; and / or (iii) the protection of the identity of reporting persons; and / or (iv) the protection of reporting persons against retaliation.

In addition, you may submit a complaint to the Data Protection Authority of the country in which the subsidiary of the Group acting as your employer has its registered seat.