

INFORMATION NOTICE ON THE PROCESSING OF PERSONAL DATA, PURSUANT TO ARTICLES 13 AND 14 OF REGULATION (EU) 2016/679 ("GDPR") DERIVING FROM THE SYSTEM ADOPTED BY THE COMPANY TO COLLECT REPORTS OF ILLEGAL CONDUCT RELEVANT PURSUANT TO LEGISLATIVE DECREE NO. 231/2001 AND VIOLATIONS OF THE ORGANISATION, MANAGEMENT AND CONTROL MODEL

	<p>DATA CONTROLLER</p>	<p>ALVAPACK S.r.l. Via Marconi, 32 – 40122, Bologna (BO) VAT No. 02402701201 Email address info@alvapack.it (hereinafter referred to as the “Company” or “Data Controller”)</p>
---	-------------------------------	---

TYPE OF DATA PROCESSED AND SOURCE OF DATA	
	<p>The Company allows detailed reports to be made of:</p> <ul style="list-style-type: none"> • unlawful conduct constituting the predicate offences referred to in Legislative Decree No. 231/2001; • violations of the Organisation, Management and Control Model adopted pursuant to Legislative Decree no. 231/2001 (hereinafter, OMC), the Operating Procedures referred to therein and the Company's Code of Ethics. <p>Reports may be named or anonymous.</p> <p>Using the <i>online</i> reporting form, accessible from the Company's website (https://alvapack.it/whistleblowing/), the reporting party may provide their personal data in the case of named reports (specifically, personal details and contact details), information relating to their relationship with the Data Controller, the circumstances and description of the event being reported, as well as the personal data of the reported party and/or any third parties (hereinafter, "Data").</p> <p>Any data provided by the reporting party is supplied directly by the reporting party (and therefore acquired by the Data Controller from the data subject pursuant to Article 13 of the GDPR); data relating to the reported party and/or third parties is supplied by the reporting party (and therefore acquired by the Data Controller from third parties pursuant to Article 14 of the GDPR).</p> <p>No special categories of Data (e.g. data relating to health) are requested by the Data Controller. If shared by the reporting party, the Data will only be processed if one of the conditions set out in Article 9 of the GDPR applies, as indicated below; if these conditions do not apply, the Data will be deleted immediately. The same considerations also apply to any judicial data (e.g. data relating to alleged offences) that may be provided, which will be processed in accordance with Article 10 of the GDPR.</p>

	PURPOSE OF PROCESSING		LEGAL BASIS FOR PROCESSING		DATA RETENTION PERIOD
	<p>Management of detailed reports of unlawful conduct or violations of the MOG, made in writing and orally, including preliminary investigations to verify the validity of the reported facts and the adoption of consequent measures in accordance with the provisions of the MOG and/or irregularities in pre-contractual, contractual, probationary period with the Data Controller or after the termination of the legal relationship if the information on the violations was acquired during the course of the same legal relationship.</p>		<p>The Data are processed to fulfil a legal obligation to which the Data Controller is subject pursuant to Legislative Decree no. 231/2001, as amended by Law no. 179/2017, as well as EU Directive no. 2019/1937 as implemented by Legislative Decree no. 24/2023, Art. 6 (1) letter c) of the GDPR.</p> <p>The processing, if any, of special categories of data is based on the fulfilment of obligations and the exercise of specific rights of the Data Controller and the data subject in the field of labour law pursuant to Art. 9, para. 2, letter b) of the GDPR.</p> <p>Any data relating to criminal convictions and offences will only be processed in cases where this is required by law pursuant to Art. 10 of the GDPR.</p>		<p>The Data shall be stored for the time necessary to process the report and, in any case, for no longer than 5 years from the date of notification of the final outcome of the reporting procedure, in compliance with the confidentiality obligations set out in Article 12 of Legislative Decree No. 24/2023 and the principle set out in Article 5, paragraph 1, letter e) of the GDPR.</p> <p>If the report leads to litigation or disciplinary proceedings against the reported party or the reporter, the Data will be retained for the entire duration of the litigation or out-of-court proceedings until the expiry of the time limits for bringing an appeal.</p> <p>Exceptions to the above five-year retention period are reports whose contents are completely unrelated to the purposes of the whistleblowing channel, which will be deleted within two months of completion of the analysis, documenting the reasons why they were not considered relevant.</p>
	<p>If necessary, to ascertain, exercise or defend the rights of the Data Controller in court.</p>		<p>Where the processing involves the collection of special categories of personal data pursuant to Article 9 of the GDPR (e.g. data concerning health, racial or ethnic origin, political opinions, etc.) or judicial data pursuant to Article 10 of the GDPR (e.g. data relating to criminal proceedings or alleged offences), such information will be processed by exclusively within the limits permitted by current legislation, on the basis of appropriate grounds of</p>		<p>The Data will be retained for the entire duration of the legal proceedings or until the expiry of the time limits for appeal.</p>

	lawfulness and adopting adequate measures to ensure its security and confidentiality.	
--	---	--

Once the above retention periods have expired, the Data will be destroyed, deleted or anonymised, in accordance with the technical procedures for deletion, backup and accountability of the Data Controller.



MANDATORY PROVISION OF DATA

The provision of personal data is optional. In particular, failure to provide the reporting person's identification details will result in the report being treated as anonymous.

However, the information contained in the report (e.g. the circumstances and description of the facts reported, with any references to the reported person and/or third parties) is necessary to enable the Data Controller to verify the report and take any measures against the reported person.

The Data Controller does not require the provision of special categories of personal data (Article 9 of the GDPR) or judicial data (Article 10 of the GDPR); if such data is voluntarily provided by the reporting party, it may only be processed if the conditions of lawfulness provided for by current legislation are met.

In the absence of such conditions, the data will be deleted without delay.



METHOD OF PROCESSING

The processing of Data, both with reference to written and oral reports, will be carried out using paper, electronic or automated means with logic related to the purposes indicated above and, in any case, in such a way as to guarantee the security and confidentiality of the Data itself. Specific security measures are observed to prevent the loss of Data, illicit or incorrect use and unauthorised access. In cases where a face-to-face meeting is requested, the meeting will be documented, with prior consent, by the staff in charge by means of a report.



DATA RECIPIENTS

The Data may be disclosed to parties acting as Data Controllers, such as, for example, judicial authorities and other public entities entitled to request it, as well as individuals, companies, associations or professional firms that provide assistance and advice on the matter in compliance with the confidentiality obligations set out in Article 12 of Legislative Decree No. 24/2023.

In exceptional cases, if the Company initiates disciplinary proceedings against the reported person based solely on the report, the whistleblower's Data may be disclosed to the reported person, exclusively to enable the latter to exercise their right of defence in compliance with the confidentiality obligations set out in Article 12 of Legislative Decree No. 24/2023.

PERSONS AUTHORISED TO PROCESS DATA



The Data may be processed by authorised personnel, members of the Supervisory Body and investigators involved in the management of reports, acting on the basis of specific instructions regarding the purposes and methods of processing and who will in any case only be involved in strictly necessary cases, taking care to preserve the absolute confidentiality of the data subjects.



TRANSFER OF DATA TO NON-EU COUNTRIES

No transfer of Data outside the European Economic Area (EEA) is envisaged in relation to the processing in question.

If, for technical and/or operational reasons, it is necessary to use entities located outside the EEA, or if it is necessary to transfer some of the data collected to technical systems and services managed in the cloud and located outside the EEA, the processing will be regulated in accordance with the provisions of Chapter V of the GDPR.



RIGHTS OF THE DATA SUBJECT AND COMPLAINTS TO THE SUPERVISORY AUTHORITY

The data subject may check the status of their report. In the case of anonymous reports, it is not possible to exercise the rights referred to in this paragraph, as the exercise of these rights requires the identification of the data subject in order to follow up on them.

In the case of named reports, by contacting the Company by e-mail at info@alvapak.it, data subjects may ask the Data Controller for access to the Data concerning them, their erasure in the cases provided for in Article 17 of the GDPR, the rectification of inaccurate data, the integration of incomplete data, the restriction of processing in the cases provided for in Article 18 of the GDPR, as well as the right to object to processing, for reasons related to their particular situation, in cases of legitimate interest of the Data Controller.

In the case of a direct meeting, at the request of the reporting person, the report (drawn up with the consent of the reporting person) may be verified, corrected and confirmed by the latter by means of their signature. In the case of an oral report, the express consent of the reporting person will be required and, in the case of a transcription of the oral report, it will be possible to verify, correct or confirm the content of the transcription by means of their signature.

Data subjects have the right to lodge a complaint with the competent supervisory authority in the Member State in which they habitually reside or work or in the State in which the alleged infringement occurred.

Pursuant to Article 2-undecies of Legislative Decree No. 196/2003, as amended by Legislative Decree No. 101/2018 (hereinafter, the "Code"), the rights referred to in Articles 15 to 22 of the GDPR cannot be exercised if the exercise of such rights could result in actual and concrete prejudice to the confidentiality of the identity of the employee who reports unlawful conduct of which he or she has become aware by virtue of his or her position.

In such cases, the rights in question may be exercised through the Data Protection Authority (in accordance with the procedures set out in Article 160 of the Code), which shall inform the data subject that it has carried out all the necessary checks or reviews, as well as of the data subject's right to seek judicial review.