


DISCLOSURE RELATING TO THE PROCESSING OF PERSONAL DATA PURSUANT TO ARTICLES 13 AND 14 OF REGULATION (EU) 2016/679 (“GDPR”) RESULTING FROM THE SYSTEM ADOPTED BY THE COMPANY TO COLLECT REPORTS OF ILLEGAL CONDUCT OR VIOLATIONS OF THE ORGANISATION, MANAGEMENT AND CONTROL MODEL PURSUANT TO LEGISLATIVE DECREE NO. 231/2001 AND THE REPORTS COVERED UNDER LEGISLATIVE DECREE NO. 24/2023

	DATA CONTROLLER	Friulchem S.p.A. Address: Via San Marco 23, Vivaro (PN), 33099 - Italy Email address: privacy@friulchem.com (hereinafter also the “Company” or the “Data Controller”).
---	------------------------	---




TYPE OF DATA PROCESSED AND THE SOURCE OF DATA	
	<p>The Company makes it possible to make detailed written or oral reports relating to:</p> <ul style="list-style-type: none"> • unlawful conduct of an administrative, accounting, civil or criminal nature, including in accordance with Legislative Decree No. 231/2001; • violations of the Company’s internal provisions, including, where present: <ul style="list-style-type: none"> - the Code of Ethics; - the Organisation, Management and Control Model adopted by the Company pursuant to Legislative Decree No. 231/2001 and related procedures; - national collective bargaining agreements; - internal regulations (procedures, policies, operating instructions, etc.); • breaches of European provisions consisting of: <ul style="list-style-type: none"> - acts and omissions that harm the financial interests of the European Union; - acts and omissions affecting the internal market; - acts and conduct that defeat the object or purpose of the provisions of the acts of the European Union in the areas referred to above; • violations of national and EU provisions consisting of unlawful acts concerning – by way of example but not limited to – the following sectors: <ul style="list-style-type: none"> - public contracts; - financial services, products and markets and prevention of money laundering and terrorist financing; - product safety and compliance; - transport safety; - environmental protection; <p>digitally, through its whistleblowing platform.</p> <p>Reports may be made either by name or anonymously:</p> <ul style="list-style-type: none"> • in the case of anonymous reports, the company’s IT systems will not be able to identify the whistleblower from the portal access point (IP address);

- in the case of named reports, written or oral, at the whistleblower’s choice his or her personal data will be associated with the report. In the case of named reports, the whistleblower may use the form made available on the whistleblowing platform, indicating his or her data (specifically, personal data and contact details), information relating to his or her relationship with the Data Controller, the circumstances and description of the matter reported, and the personal data of the reported party and/or of any third parties (hereinafter the “**data**”).


The whistleblowing platform also provides the possibility, on an entirely optional basis, for the whistleblower to make reports by voice recording, subject to express consent, in which case the data collected will also include the voice of the whistleblower. The whistleblowing platform also allows the whistleblower, at his or her request, to schedule a direct meeting with the Company departments appointed and expressly authorised to process data and who have received adequate operating instructions. The meeting, with the prior consent of the whistleblower, will be specifically documented.


Any whistleblower data indicated are provided directly by the whistleblower (and therefore acquired by the Data Controller from the interested party pursuant to Article 13 of the GDPR). The data of the reported party and/or third parties are provided by the whistleblower (and therefore acquired by the Data Controller from third parties pursuant to Article 14 of the GDPR).


Furthermore, in the context of this activity, special data (for example, relating to health) and judicial data (in particular, relating to cases of crime) may also be processed if they are directly provided by the whistleblower. Indeed, these are not categories of data mandatorily required for the purpose of sending the report.


 PURPOSE OF DATA PROCESSING	 LEGAL BASIS FOR DATA PROCESSING	 DATA RETENTION PERIOD
<p>Management of detailed reports of illegal conduct or violations of the Organisation, Management and Control Model, carried out in written and oral form, including preliminary investigative activities aimed at verifying the validity of the reported facts and the adoption of the consequent measures in accordance with the provisions of the Organisation, Management and Control Model, illegal and/or irregular acts in the context of pre-contractual and contractual relationships, probationary period agreed upon with the Data Controller or after the dissolution of the legal relationship if the information on the violations was</p>	<p>The data are processed to comply with 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 transposed by Legislative Decree No. 24/2023, and Article 6(1)(c) of the GDPR.</p> <p>The processing, if any, of particular categories of data is based on Article 9(2)(g) of the GDPR, in accordance with the provisions of Article 2-sexies(1) of Legislative Decree No. 196/2003, as amended by Legislative Decree No. 101/2018.</p> <p>Any data relating to criminal convictions and offences will be processed only in cases</p>	<p>The data are kept for the time necessary to process the report and in any case for no longer than 5 years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations referred to in Article 12 of Legislative Decree No. 24/2023 and the principle referred to in Article 5(1)(e) of the GDPR.</p> <p>If the report involves the establishment of a dispute or disciplinary proceeding against the reported person or the whistleblower, the data will be kept for the entire duration of the dispute or out-of-court proceeding until the expiry of</p>


<p>acquired during the same legal relationship as provided for by Legislative Decree No. 24/2023.</p>	<p>where it is required by law pursuant to Article 10 of the GDPR.</p> <p>With reference exclusively to the making of reports by voice recording, the recording will be processed with the express consent of the whistleblower, pursuant to Article 14 of Legislative Decree No. 24/2023.</p>	<p>the terms of applicability of the appeal proceedings.</p>
<p>If necessary, to ascertain, exercise or defend the rights of the Data Controller in court.</p>	<p>Legitimate interest of the Data Controller pursuant to Article 6(1)(f) of the GDPR.</p> <p>Any categories of special data will be processed to ascertain, exercise or defend a right in court pursuant to Article 9(2)(f) of the GDPR.</p> <p>The processing of data relating to criminal convictions and offences, if any, will be processed only in cases where it is required by law pursuant to Article 10 of the GDPR.</p>	<p>The data will be kept for the entire duration of the judicial proceedings or until the expiry of the appeal periods.</p>
<p>Once the data retention periods indicated above have expired, the data will be destroyed, deleted or made anonymous, compatible with the technical cancellation, backup and accountability procedures of the Data Controller.</p>		


	<p>OBLIGATION TO PROVIDE DATA</p>
	<p>The provision of data is optional.</p> <p>In particular, in the event of failure to provide the whistleblower’s identification data, the report will be made anonymously. The information provided in the report (e.g. the circumstances and the description of the fact subject to the report with reference to the reported party and/or third parties) are necessary to allow the Data Controller to acquire, manage and initiate any preliminary investigation phase pursuant to Legislative Decree No. 231/2001 as amended, Legislative Decree No. 90/2017 as amended, and Legislative Decree No. 24/2023.</p> <p>Particular categories of data and/or judicial data are not required by the Data Controller and may be processed, if sent by the whistleblower, only in the presence of the conditions listed above. In the absence of such conditions, they will be promptly deleted.</p>

	<p>DATA PROCESSING METHODS</p>
	<p>The processing of data, both with reference to written and oral reports, will take place through paper, electronic or automated tools (whistleblowing platform) with logics related to the purposes indicated above and, in any case, in such a way as to guarantee the security and confidentiality of the data. Specific security measures are observed to prevent the loss of data, as well as illicit or incorrect use thereof and unauthorised access thereto. In cases where a direct meeting is requested by the whistleblower, subject to consent this may be documented by means of minutes taken by the staff appointed.</p>

	DATA RECIPIENTS
	<p>The data may be disclosed to parties operating as Data Controllers such as, by way of example, judicial authorities and other public entities entitled to request them, as well as persons, companies, associations or professional firms that provide assistance and advice on the subject in compliance with the confidentiality obligations referred to in Article 12 of Legislative Decree No. 24/2023.</p>
	<p>The data are also processed on behalf of the Data Controller by the provider that manages the whistleblowing platform (as well as the storage of the information and data contained therein), to which adequate operating instructions are given and who is specifically appointed as Data Processor pursuant to Article 28 of the GDPR.</p>
	<p>In exceptional cases, if the Companies initiate a disciplinary procedure against the reported party based solely on the report, the whistleblower's data may be communicated to the reported party, exclusively to exercise the latter's right of defence in compliance with the confidentiality obligations referred to in Article 12 of Legislative Decree No. 24/2023.</p> <p>The identity of the party reported and of the persons mentioned in the report are protected until the conclusion of the proceedings initiated by reason of the report in compliance with the same guarantees provided in favour of the whistleblower.</p>

	PARTIES AUTHORISED TO PROCESS DATA
	<p>The data may be processed by the members of the Direct Channel, the Alternative Channel, as well as by staff, members of the Supervisory Body and internal investigators involved in the management of reports who act on the basis of specific instructions regarding the purposes and methods of processing and who will in any case be involved only in strictly necessary cases, taking care to preserve the absolute confidentiality of the interested parties.</p>

	TRANSFER OF DATA TO NON-EU COUNTRIES
	<p>With regard to the data processing in question, there are no transfers of data outside the European Economic Area (EEA).</p>

	RIGHTS OF THE INTERESTED PARTY – COMPLAINT TO THE SUPERVISORY AUTHORITY
	<p>The whistleblower will be able to check the status of his or her report through the whistleblowing platform. In the case of anonymous reports, it will not be possible for the whistleblower to exercise the rights referred to in this section, as the exercise of rights implies the identification of the interested party.</p>
	<p>By contacting the Company via email at privacy@friulchem.com, interested parties may request that the Data Controller provide access to the data concerning them, their deletion in the cases provided for under Article 17 of the GDPR, the rectification of inaccurate factual data, the integration of incomplete data, the limitation of processing in the cases provided for under Article 18 of the GDPR, as well as opposition to processing, for reasons related to their particular situation, in cases of legitimate interest of the Data Controller.</p>

	<p>In the event of a direct meeting, at the request of the whistleblower, the report (drawn up with the consent of the whistleblower) may be verified, rectified and confirmed by the latter with his or her signature. In the case of an oral report, the express consent of the whistleblower will be required and, in the case of a transcript of the oral report, it will be possible to verify, correct or confirm the content of the transcript with his or her signature.</p>
	<p>Interested parties 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.</p>
	<p>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 this may result in an effective and concrete prejudice to the confidentiality of the identity of the employee who reports illegal conduct of which he or she has become aware by reason of his or her role.</p> <p>In this case, the rights in question may be exercised through the supervisory authority (in the manner referred to in Article 160 of the Code), which informs the interested party that it has carried out all the necessary checks or has carried out a review, as well as the right of the interested party to lodge a judicial appeal.</p>