

Privacy Notice – Whistleblowing

We, Mölnlycke Health Care, are responsible as data controller for the processing of your personal data when you use or appear in a report within our internal whistleblowing system.

For the purposes of this privacy notice, "**Mölnlycke**" means the parent company Mölnlycke AB, a company incorporated in Sweden under company registration number 556723-5949 and companies wholly or partially controlled by Mölnlycke AB, which is thus part of the same group, including Mölnlycke Health Care AB with company registration number 556547-5489, Mölnlycke Holding AB with company registration number 556693-6729, Mölnlycke Health Care N.V with company registration number BE 0462556475, Mölnlycke Health Care Klinipro S.R.O. with company registration number CZ25886665, Mölnlycke Health Care ProcedurePak sro with company registration number CZ 02948231, Mölnlycke Health Care OY with company registration number 02074652, Mölnlycke Health Care SAS with company registration number 383197472, Mölnlycke Health Care GmbH with company registration number HRB 13965, Mölnlycke Health Care SRL with company registration number IT 12300580151, Mölnlycke Health Care SL with company registration number B61526414, Mölnlycke Health Care Polska SP z.o.o. with company registration number 050832291.

All references in this personal data notice to "**we**", "**us**" and "**our**" shall be considered a reference to Mölnlycke. You can find our contact information at the end of this privacy notice.

We respect your privacy and are committed to protecting your personal data.

Scope of this Privacy Notice

This privacy notice applies to Mölnlycke's processing of personal data regarding users of, and individuals who are subject to reporting within the internal whistleblowing channel or figures as a suspect or witness of a reported incident. This Privacy Notice contains, *inter alia*, information regarding the purposes for which we process personal data, with whom we share your information and what rights you have in relation to your personal data.

What categories of personal data do we process, for what purpose and on what legal basis do we base our processing of personal data?

Mölnlycke processes personal data in the manner and for the purposes described in the tables below. The tables below also show the legal basis on which Mölnlycke bases its processing for each purpose and for how long we will retain your personal data.

What we do and why:	The personal data that we process:
We handle reports received through the whistleblowing channel by collecting and administering the reports. We will also communicate with the persons who the reports concern, including alleged witnesses of the reported incident. We will	<ul style="list-style-type: none">• Contact information, such as name, telephone number, address and e-mail address.• Birthdate.• Report history and report number.• Employment information (such as job title and role).• Pictures and audio recordings.

<p>handle, follow-up and document the content of the report and any upcoming questions. We will do this in order to be able to properly handle all whistleblowing reports concerning violations of the law.</p>	<ul style="list-style-type: none"> • Personal data related to criminal convictions, suspicion of and/or actual violations of the law in the form of violations of, for example, the Money Laundering Act.
<p>Our legal basis for processing:</p>	
<p>Legal obligation: The processing of your personal data is required by law. If the personal data is not processed, our legal obligation cannot be fulfilled.</p>	
<p>How we share and transfer your data:</p>	
<p>In order to fulfil the purposes stated above, Mölnlycke will share your personal data with the following recipients;</p> <ul style="list-style-type: none"> • With external lawfirm Setterwalls on a regular basis and with other external counsels on a case by case basis. • With data forensics experts or other experts on a case by case basis • relevant authorities, and • IT provider of Whistleblowing channel Convercent by OneTrust <p>to the extent it is necessary for them to perform their services to us.</p> <p>Mölnlycke will not transfer your personal data to a country outside the European Union (“EU”)/European Economic Area (“EEA”) within the scope of this processing activity.</p>	
<p>How long we keep your data:</p>	
<p>We process your personal data during the storage period required by law or otherwise during the time it is necessary for the establishment, exercise or defence of legal claims.</p>	

<p>What we do and why:</p>	<p>The personal data that we process:</p>
<p>We will conduct investigations of misconduct and suspected offenses committed within Mölnlycke's organization in the form of suspected or actual violations of law, with the purpose to properly handle all suspected violations of law within Mölnlycke's organization. To achieve this we will handle, follow up and document whistleblower reports</p>	<ul style="list-style-type: none"> • Contact information, such as name, telephone number, address and e-mail address. • Birthdate. • Report history and report number. • Employment information (such as job title and role). • Pictures and audio recordings.

<p>contents and upcoming questions. We will collect and review information from the IT-equipment and the digital systems you use within your employment and that Mölnlycke controls. We will also interview relevant persons within the investigation, including alleged witnesses of the reported incident and contact the relevant authorities for the investigation.</p>	<ul style="list-style-type: none"> • Communication history. • Internet history. • User history from the IT-equipment and digital systems that you as an employee use within the framework of your employment and that Mölnlycke controls. • Personal data related to criminal convictions, suspicion of and/or actual violations of the law in the form of violations of, for example, the Money Laundering Act.
<p>Our legal basis for processing:</p>	
<p><i>Legal obligation:</i> The processing of your personal data is required by law. If the data is not processed, our legal obligation cannot be fulfilled.</p>	
<p>How we share and transfer your data:</p>	
<p>In order to fulfil the purposes stated above, Mölnlycke will share your personal data with the following recipients;</p> <ul style="list-style-type: none"> • With external lawfirm Setterwalls on a regular basis and with other external counsels on a case by case basis. • With data forensics experts or other experts on a case by case basis • relevant authorities, and • IT provider of Whistleblowing channel Convercent by OneTrust <p>to the extent it is necessary for them to perform their services to us.</p> <p>Mölnlycke will not transfer your personal data to a country outside the European Union (“EU”)/European Economic Area (“EEA”) within the scope of this processing activity.</p>	
<p>How long we keep your data:</p>	
<p>We process your personal data for the storage period required by law or otherwise for the time necessary for the establishment, exercise or defence of legal claims.</p>	

<p>What we do and why:</p>	<p>The personal data that we process:</p>
<p>We will handle reports of violations of internal policies through collecting and administering reports received through the whistleblowing channel. We will also</p>	<ul style="list-style-type: none"> • Contact information, such as name, telephone number, address and e-mail address. • Birthdate.

<p>communicate with the persons who the reports concern, including alleged witnesses of the reported incident. We will handle, follow-up and document the content of the report and any upcoming questions. We will do this in order to be able to properly handle all whistleblowing reports concerning potential violations of internal policies.</p>	<ul style="list-style-type: none"> • Registration history and registration number. • Employment information (such as job title, employee identifier and role of responsibility). • Pictures and audio recordings. • Personal data related to actions in violation of Mölnlycke's Code of Conduct and internal policies.
<p>Our legal basis for processing:</p>	
<p><i>Legitimate interest:</i> The processing is necessary to fulfil our legitimate interest in ensuring that our internal policies for our business are complied with.</p>	
<p>How we share and transfer your data:</p>	
<p>In order to fulfil the purposes stated above, Mölnlycke will share your personal data with the following recipients;</p> <ul style="list-style-type: none"> • With external lawfirm Setterwalls on a regular basis and with other external counsels on a case by case basis. • With data forensics experts or other experts on a case by case basis • relevant authorities, and • IT provider of Whistleblowing channel Convercent by OneTrust <p>to the extent it is necessary for them to perform their service to us.</p> <p>Mölnlycke will not transfer your personal data to a country outside the European Union (“EU”)/European Economic Area (“EEA”) within the scope of this processing activity.</p>	
<p>How long we keep your data:</p>	
<p>For this purpose, we will process your personal data until the investigation case is completed and for the time necessary to establish, exercise or defend legal claims.</p>	

<p>What we do and why:</p>	<p>The personal data that we process:</p>
<p>We will investigate misconduct and suspected offenses within Mölnlycke's organization in the form of violations of internal policies. To achieve this we will handle, follow up and document whistleblower reports contents and</p>	<ul style="list-style-type: none"> • Contact information, such as name, telephone number, address and e-mail address. • Birthdate. • Report history and report number.

<p>upcoming questions. We will collect and review information from the IT-equipment and the digital systems you use within your employment and that Mölnlycke controls. We will also interview relevant persons within the investigation, including alleged witnesses of the reported incident and contact the relevant authorities for the investigation.</p>	<ul style="list-style-type: none"> • Employment information (such as job title and role). • Pictures and audio recordings. • Communication history. • Internet history. • User history from the IT-equipment and digital systems that you as an employee use within the framework of your employment and that Mölnlycke controls. • Personal data related to actions in violation of Mölnlycke1's Code of Conduct and internal policies.
<p>Our legal basis for processing:</p>	
<p><i>Legitimate interest:</i> The processing is necessary to fulfil our legitimate interest in ensuring that our internal policies for our business are complied with.</p>	
<p>How we share and transfer your data:</p>	
<p>In order to fulfil the purposes stated above, Mölnlycke will share your personal data with the following recipients;</p> <ul style="list-style-type: none"> • With external lawfirm Setterwalls on a regular basis and with other external counsels on a case by case basis. • With data forensics experts or other experts on a case by case basis • relevant authorities, and • IT provider of Whistleblowing channel Convercent by OneTrust <p>to the extent it is necessary for them to perform their service to us.</p> <p>Mölnlycke will not transfer your personal data to a country outside the European Union (“EU”)/European Economic Area (“EEA”) within the scope of this processing activity.</p>	
<p>How long we keep your data:</p>	
<p>For this purpose, we will process your personal data until the investigation case is completed and for the time necessary to establish, exercise or defend legal claims.</p>	

From where do we collect your personal data?

Mölnlycke processes personal data that is collected directly from you when you use the whistleblowing system, or that is stated by another person within the scope of a report.

Transfer of personal data outside of EU/EEA?

We strive to always process your personal data within the EU or EEA. However, if we transfer your personal data, in accordance with what is stipulated in the tables above, to service providers who, either themselves or by their sub-contractors, are located or have business activities in a country outside the EU or EEA. In such cases, we are responsible for ensuring that the transfer is made in accordance with applicable data protection legislation before it occurs, e.g. by ensuring that the country in which the recipient is located ensures an adequate level of data protection according to the European Commission, or by ensuring appropriate safeguards based on the use of standard contractual clauses that the European Commission has adopted and other appropriate measures to safeguard your rights and freedoms.

You may access a list of the countries that the European Commission has decided provide an adequate level of data protection at this [link](#).

You may access the European Commission's standard contractual clauses at this [link](#).

Your rights

In this section we describe your rights as a data subject. You can exercise them by contacting us using the contact information at the end of this document. Please note that not all rights listed below are absolute and there are exemptions which can be valid. Your rights are the following:

- *Right of access*

You have the right upon request to get a copy of your personal data which we process and to get complementary information regarding our processing of your personal data.

- *Right of rectification*

You have the right to have your personal data rectified and/or complemented if they are wrong and/or incomplete.

- *Right to erasure*

You have the right to request that we erase your personal data without undue delay in the following circumstances: (i) the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed; (ii) you withdraw your consent on which the processing is based (if applicable) and there is no other legal ground for the processing; (iii) you object to our processing of personal data, and we do not have any overriding legitimate grounds for the processing; (iv) the processed personal data is unlawfully processed; or (v) the processed personal data has to be erased for compliance with legal obligations.

- *Right to restriction*

You have the right to restrict the processing of your personal data in the following circumstances: (i) you contest the accuracy of the personal data during a period enabling us to verify the accuracy of such data; (ii) the processing is unlawful, and you oppose erasure of the personal data and request restriction instead; (iii) the personal data is no longer needed for the purposes of the processing, but are necessary for you for the establishment, exercise or defence of legal

claims; or (iv) you have objected to the processing of the personal data, pending the verification whether our legitimate grounds for our processing override your interests, rights and freedoms.

- *Right to data portability*

If your personal data has been provided by you and our processing of your personal data is based on your consent or on the performance of a contract with you, you have the right to receive the personal data concerning you in a structured, commonly used and machine-readable format in order to transmit these to another service provider where it would be technically feasible and can be carried out by automated means.

- *Right to object*

You have the general right to object to our processing of your personal data when it is based on our legitimate interest. If you object and we believe that we may still process your personal data, we must demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or for the establishment, exercise or defence of legal claims.

- *Right to object to direct marketing*

You have the right to at any time object to processing which is done for the purpose of direct marketing. If you object to such processing, we will no longer process your data for such purposes.

- *Right to withdraw consent*

When our processing of your personal data is based on your consent, you have the right to withdraw your consent at any time. Please note that the lawfulness of any processing based on your consent before its withdrawal is not affected by the withdrawal.

Complaints to the supervisory authority

The data protection authority in Sweden is 'Integritetsskyddsmyndigheten'. If you believe that our processing is performed in breach of applicable data protection legislation, we encourage you in first-hand to contact us in order for us to oversee your complaints. You may at any time also file a complaint with the supervisory authority.

Contact us

If you have any questions about the processing of your personal data or want to exercise any of your rights, please contact us at:

Phone number: +46 31 722 30 00

E-mail: privacy@molnlycke.com

Mölnlycke AB,

c/o Mölnlycke Health Care AB

Box 13080 402 52 Göteborg SWEDEN