

Global privacy commitment

At Mölnlycke, we respect people's privacy and it is important for us to process personal data ethically and responsibly, both as an employer and as a trusted business partner.

Applicable data protection laws regulate the way Mölnlycke collects and processes personal data. Our internal privacy policies and procedures also require us to meet legal obligations around privacy in the jurisdictions where we operate. Data protection laws apply to all processing of personal data by Mölnlycke.

Complying with these laws is essential to ensure that Mölnlycke operates in an ethical and responsible manner. We respect the privacy and rights of individuals whose personal data is processed by our company, regardless of whether they are customers, business partners, healthcare professionals, employees, or patients.

What is personal data?

Personal data can be any type of information which is related to an identified or identifiable individual.

Examples of personal data are:

- Name and surname of a person or a person's email address such as name.surname@molnlycke.com,
- A person's home address or their location data (for example collected via functions on a mobile phone),
- An Internet Protocol (IP) address or any other type of identifier of a personal device,
- Images enabling identification of a person,
- A person's health data.

Sometimes, personal information is changed in a way that hides who it belongs to, like using a code or a fake name. But even when it is changed like this, if it can still be used to figure out who the person is, it is still considered personal information. However, when data is completely changed so that it can't be linked back to any individual, like when it is grouped together or turned into statistics, it is not covered by these rules.

1. Purpose and scope

The aim of this Privacy Commitment is to establish the global and fundamental principles guiding Mölnlycke's protection of individuals' rights to their personal data and integrity. These principles shape Mölnlycke's policies and procedures, extending across the entire organization and also to its business partners.

This Privacy Commitment applies across the entire Mölnlycke organization, including its work methods, processes, materials, equipment, software, communication channels, and paper documents involved in handling personal data.

2. Ethical and lawful processing of Personal Data

We believe that privacy is more than just following the law. As a world leading medical solutions company, we have an ethical responsibility – in addition to the legal obligations – to ensure sustainable use of, and to protect, the personal data entrusted to us. It is part of Mölnlycke being an ethical and sustainable business, revolutionising care for people and planet. All Mölnlycke personnel are expected and obliged to respect and honour this Privacy Commitment as well as Mölnlycke's internal policies and procedures of handling personal data, to ensure that the processing of personal data is ethical, lawful, fair, and transparent, and that the rights of the data subjects are duly fulfilled and respected. To this end, Mölnlycke operates under a set of general good practices in relation to personal data processing, safeguarding that:

- i. the processing of personal data is:
 - fair to the individuals whose personal data we are processing;
 - carried out in accordance with other applicable law(s);
 - carried out based on a valid and documented legal basis;
 - only carried out within the scope of the specific purposes for which such personal data was collected, or for lawful compatible secondary purposes (e.g., legitimate scientific research), if we collect a new consent, or to comply with a legal obligation;
- ii. we are clear, open, and honest with individuals about how their personal data will be used;
- iii. to the extent possible, all individuals shall receive information about the processing of their personal data in a clear, transparent, and prompt manner;
- iv. the collection, use and storage of personal data is carried out only on the minimum personal data, necessary and sufficient for the respective purpose;
- v. the personal data processed is accurate;
- vi. personal data is only stored for the period of time necessary to fulfil the purpose for which it was collected, to comply with a legal obligation, or for a lawful compatible secondary use, and is subsequently anonymised or deleted, in accordance with Mölnlycke's retention and deletion policy;

- vii. personal data is kept centralized whenever possible to ensure quick and efficient fulfilment of data subjects' rights;
- viii. any personal data transferred cross-borders is adequately safeguarded and protected;
- ix. a record of data processing activities is maintained to establish a transparent overview of the processing activities conducted by or on behalf of Mölnlycke; and,
- x. personal data is processed in a way that safeguards security, integrity, and confidentiality of the personal data.

3. Mölnlycke's governance and security measures

Data Protection Officer (DPO). Mölnlycke appoints a global, as well as local DPOs, where applicable and required, which are registered with the competent supervisory authority. The DPOs are responsible for overseeing that all processing activities are conducted in compliance with applicable data protection laws, this Privacy Commitment, and other Mölnlycke policies and procedures. In addition, the DPOs are responsible for the training of personnel as well as functioning as the point of contact for inquiries from individuals whose personal data Mölnlycke process, or from the supervisory authorities.

Cross-border transfers. Mölnlycke is a global company and therefore processes personal data within the different jurisdictions that Mölnlycke operates. We will not transfer personal data across borders if not necessary for the purpose of processing. When personal data is processed by Mölnlycke within the EU/EEA, we strive to limit any third country transfers. If Mölnlycke would transfer personal data outside of EU/EEA, Mölnlycke will safeguard that the transfer is made in accordance with applicable data protection laws, 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 the rights and freedoms of individuals.

Retention policy. Mölnlycke maintains a policy and procedures to safeguard that personal data is either anonymised or deleted when it is no longer necessary for the purpose it is processed. Mölnlycke strives to foster a culture of "deciding what to keep" instead of "deciding what to delete".

Records of processing activities. Mölnlycke maintains a clear and transparent record of all processing activities. This enables Mölnlycke to have an updated overview of the business activities which involves the processing of personal data and ensuring that such activities are conducted in a compliant manner.

Incident management. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. If a personal data breach would occur, Mölnlycke is prepared to handle it through its established policies and routines on identification, remedial, assessment, reporting and documentation of breaches.

Data protection by design and by default. At Mölnlycke, the principles of privacy and compliance with applicable data protection laws is a natural part of the development of any project, process, or product, involving the processing of personal data. This includes implementing necessary technical and organisational measures to safeguard that the processing activities are carried out in an ethical manner and in compliance with applicable law, this Privacy Commitment, and any other Mölnlycke policy or procedure. Mölnlycke's operations are certified according to applicable standards and maintains all necessary routines and procedures as required according to such certifications.

Further examples of such technical and organisational measures are:

Pseudonymisation. All personal data processed by or on behalf of Mölnlycke is pseudonymised to the extent possible. This means that information that can directly identify an individual, such as name, is removed.

Encryption. Personal data is protected in accordance with Mölnlycke's routines on information classification. When necessary, the personal data is encrypted in transit, rest, and use.

Firewalls. Robust firewalls are established to function as a barrier and protect Mölnlycke's digital assets and environment.
Automated reminders and security checks.
Mölnlycke's digital systems provide automated reminders for e.g., retention periods.

Access control. Role-based access control safeguards that personal data is only accessible by personnel who has a legitimate need to process such personal data.

Contractual obligations. Any and all contracts entered into by or on behalf of Mölnlycke, which involves processing of personal data, contains obligations in relation to data protection.

Training/education. All personnel are trained in how to handle personal data in compliance with the applicable data protection laws. Personnel working specifically with processing of sensitive personal data receives additional and targeted training.

Personnel privacy champions. As a global world-leading MedTech company, Mölnlycke acknowledges the need of establishing employee privacy champions of the business, to be able to excel the level of privacy compliance across the different business areas and functions.

Confidentiality. All employees, suppliers, partners, and others who can access or view personal data, or that processes personal data on Mölnlycke's behalf, are contractually bound by confidentiality. The obligation of confidentiality shall remain in force, even after termination of duties, for as long as necessary to comply with the law.

If you have questions regarding the content of this Privacy Commitment or Mölnlycke's processing of personal data, please reach out to Mölnlycke's Chief Privacy Officer at privacy@molnlycke.com.