Getinge Global Policy

# Data Privacy Global Policy

| | |
|---|---|
| Document owner | Anna Romberg |
| Version | v3 |
| Adopted by the Board of Directors | 26 April 2023 |

## 1. Summary

The objective of this Global Data Privacy Policy ("**Global Policy**") is to set out the main data privacy requirements and provide Getinge management, employees and consultants with guidelines in their daily work involving Processing of Personal Data.

Getinge is committed to Processing Personal Data in accordance with applicable data protection laws and regulations. Privacy shall always be a top priority in our daily operations.

This Global Policy applies to all employees, directors and business partners acting on behalf of Getinge.

## 2. Definitions

In this Global Policy, the following terms have the following meaning:

| | |
|---|---|
| **Data Controller** | A legal entity which alone or jointly with other entities determines the purposes and the means of the Processing of Personal Data. |
| **Data Processor** | A legal entity which Processes Personal Data on behalf of a Data Controller. |
| **Data Protection Impact Assessment** | A systematic process for evaluating a project, process or solution in terms of its impact upon data protection. |
| **Data Protection Laws** | Any and all applicable data protection laws and regulations, including but not limited to the GDPR. |
| **Data Subject** | The individual person to whom the Personal Data relates. |
| **GDPR** | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and |

| | |
|---|---|
| | on the free movement of such data, and repealing the Directive 95/46/EC. |
| **Personal Data** | Any information relating to a Data Subject. A Data Subject is one who can be identified, directly or indirectly, using a name, an identification number, location data, an online identifier or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data also includes contact details of employees, such as work email addresses and contact persons. |
| **Personal Data Breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed. |
| **Processing of Personal Data** | Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alternation, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes viewing Personal Data. |
| **Special Categories of Personal Data**- | All Personal Data directly or indirectly indicating a living natural person's racial or ethnic origin, political opinions, philosophical or religious beliefs, sexual orientation, trade union membership and activities, genetic or biometric data, and data concerning health or sex life. |
| **Supervisory Authority** | An independent public authority responsible for monitoring compliance with Data Protection Laws. |

# 3. Scope and objective

This Global Policy is valid for all Getinge companies, its subsidiaries and joint operations (jointly "**Getinge**") and applies to all our employees, as well as consultants and agency personnel who work at Getinge premises or under the direction of Getinge (all referred to in this Global Policy as

"**employees**"). The general rule is that this Global Policy applies to all Processing of Personal Data within Getinge. Exceptions only apply in cases set forth in this Global Policy.

The objective of this Global Policy is to provide:

a) General knowledge about Personal Data and applicable Data Protection Laws
b) Guidance on the legal requirements that are of primary importance for Getinge
c) Requirements for Getinge when Processing Personal Data
d) Instructions that must be followed when Getinge Processes Personal Data

With this Global Policy, we commit to protecting Personal Data in accordance with Data Protection Laws.

# 4. Field of application

## Specific about applicability

This Global Policy applies to:

a) Processing of Personal Data in business processes
b) IT functions, solutions or services used to Process Personal Data
c) Tools such as Outlook, PowerPoint, Word and Excel
d) Situations when Getinge provides products or services which will include Processing of Personal Data on behalf of a third party, e.g. IT solutions provided to hospitals
e) All other situations when Getinge is either a Data Controller, Data Processor and/or Joint Controller as described in this Global Policy

Other requirements than those stated in this Global Policy may be necessary for specific operations, such as requirements concerning IT security. In addition to this Global Policy, there may be additional instructions and guidelines for Processing Personal Data applicable to specific Getinge teams.

## Applicable laws, local requirements and deviations

This Global Policy is based on European data protection laws and regulations but is relevant and applicable for all Getinge's Processing of Personal Data also outside the EU/EEA. The reasons for European data protection laws and regulations being applicable to such Processing may for example be that:

a) The Processing relates to procedures, systems, routines or decisions adopted by Getinge's headquarter, which is based within the EU/EEA
b) The Processing relates to goods and services offered to Data Subjects within the EU/EEA, or monitoring of their behavior
c) The entity outside the EU/EEA is considered to be established in the EU/EEA due to for example having employees in the EU/EEA

When local data protection laws and regulations impose requirements that are different or more stringent than those imposed by this Global Policy, Getinge shall comply with such laws and regulations. Should laws and/or regulations be in conflict with this Global Policy, the more stringent requirement shall take precedence. For further guidance, please contact the Data Privacy Team.

### Anonymized and pseudonymized data

This Global Policy does not apply to information which is *completely* anonymous, i.e. information which cannot be related back to an identifiable individual. Due to technical solutions available on today's market, there are many different ways to identify individuals by the use of the right technical tools. Note that anonymization could be complex to achieve in practice.

This Global Policy does apply to information which have undergone so-called pseudonymization, i.e. information which can be linked to an individual with the use of another set of information (such as a "key"). Pseudonymized data is still considered Personal Data.

**NOTE!**

Personal Data is not considered anonymized when data held by a Getinge company combined with other data held by another Getinge company or a third party can be related to an individual. For example, static as well as dynamic IP addresses are considered Personal Data since the IP number can be related to individuals if it is combined with information held by the internet operator. It does not matter that Getinge cannot access the information held by the third party, i.e. it is still considered Personal Data.

## 5. Responsibility for compliance

### Data Privacy Team

Getinge's Data Privacy Organization and the Data Privacy Team are described in the Data Privacy Governance Directive. The Data Privacy Team shall maintain the necessary expert knowledge within the field of data privacy.

The Data Privacy Team shall be seen as a discussion partner within Getinge and the opinion of the Data Privacy Team shall be given due weight in data privacy matters.

*See further: Data Privacy Governance Directive*

### Responsibility of Getinge companies

It is the ultimate responsibility of each Getinge company to comply with laws, regulations, internal Getinge decisions, processes and procedures outlined in this Global Policy. See also Section 19 regarding roles and responsibilities.

### Reporting risks

Getinge shall strive to comply fully with all Data Protection Laws and to proactively address and correct business practices that lead to, or potentially could lead to, violations. Each employee is encouraged and expected to report any incidents or suspicions of non-compliance, with the assurance that there will be no retaliation or other negative consequences for persons acting in good faith. Employees are expected to raise concerns of data privacy risks and/or suspected non-compliance to the Data Privacy Team. Concerns can also always be raised in accordance with Section 18.

# 6. General requirements when Getinge companies Process Personal Data as Controller or Joint Controller

## Controller

When a Getinge company Processes Personal Data, it might do so on its own initiative, determining why and how the Personal Data will be Processed. If a Getinge company determines the means (how) and the purposes (why) of the Processing of Personal Data, it is referred to as a Data Controller.

**EXAMPLE**

If Getinge collects Personal Data on its employees for the purposes of paying salaries each month, Getinge is determining the purposes and means of the Processing and is therefore considered to be the Data Controller of the Processing of Personal Data.

## Joint Controller

Under certain circumstances two or more Data Controllers can jointly determine the purposes (why) and means (how) of the Processing of Personal Data. For example, a Getinge company can share the role of Data Controller with one or more internal and/or external entities. This is referred to as joint controllership.

When there is a joint controller relationship, there is a legal requirement to enter into a joint controller agreement to determine the Data Controllers' respective responsibilities. The Getinge company shall ensure that the applicable template available on the Intranet is used.

**EXAMPLE**

If a Getinge company performs a research study together with a hospital, where the Getinge company and the hospital in collaboration determines why and how Personal Data shall be Processed within the project, the Getinge company and the hospital could be considered as joint controllers and would in such case need to enter into a joint controller agreement.

## Basic requirements for collecting and Processing Personal Data

Personal Data may only be Processed for specified, explicit and legitimate purposes. In order for the purposes to be considered legitimate, the planned Processing must, regardless of if a Data Subject has provided consent to the Processing:

a) Have a legitimate business purpose and may not violate any Data Protection Laws or other laws;
b) Be proportional and necessary to fulfil the purposes;
c) Not be used in ways that have unjustified adverse effects on the Data Subjects; and
d) Handle the Data Subjects' Personal Data only in ways that the Data Subjects would reasonably expect.

All Processing of Personal Data must be necessary to achieve the purpose of the Processing and the Data Subjects must not be misled or deceived with regards to the purposes or extent of the Processing of their Personal Data. Personal Data may not be Processed in any way incompatible

with the purposes that have been notified to the Data Subject. Furthermore, Personal Data Processed by Getinge companies shall be accurate, and when necessary, kept up to date.

## Legal basis for Processing Personal Data

### *General about legal basis*

Getinge may only Process Personal Data if at least one of the following applies:

a) **Consent.** The Data Subject has provided a prior consent to the Processing for the specified purpose(s). See below in this Section 6 regarding consent and withdrawal of consent.

b) **Legal obligation.** Getinge must Process the Personal Data to fulfil a legal obligation to which Getinge is subject (such as submitting tax income information to tax authorities).

c) **Performance of a contract.** The Processing of Personal Data is necessary for Getinge to fulfil its obligations in a contract that it has entered into with the Data Subject (such as retaining bank account details to pay salaries under an employment contract).

d) **Getinge's legitimate interest.** Getinge may Process Personal Data for legitimate purposes as part of its business (such as keeping a database of information on their customers or business partners, or collecting the names and phone numbers of emergency contacts for its employees), except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject. When this legal basis is applied, the specific interest in question must be identified and the Data Subject should be informed of such.

e) **Other.** There are other rare grounds on which Personal Data may be Processed, namely the protection of the vital interests of the Data Subject or tasks carried out in the public interest.

### *Consent and withdrawal of consent*

Consent should only be used by Getinge companies when no other legal basis can be used. If consent is applied as the legal basis, a Getinge company must be able to demonstrate that the Data Subject has provided consent to the Processing of Personal Data and that such consent is valid. Pre-ticked boxes, silence or inactivity never constitutes consent. If appropriate, separate consents should be obtained for different purposes of the Processing.

The consent shall be:

a) Given without being subject to other conditions;
b) Informed (see below in this Section regarding information to Data Subjects);
c) Provided voluntarily (the Data Subject must not feel pressured to provide consent); and
d) Specific and unambiguous (the Data Subject must be aware of the scope of the consent).

A consent must be given in writing or electronically. It must be clearly indicated if a Data Subject accepts the proposed Processing of Personal Data. Consent cannot be provided by silence or inactivity.

The Data Subject may withdraw the provided consent at any time. When consent is withdrawn, the concerned Getinge company shall stop Processing Personal Data about the Data Subject to the extent the Processing is based on consent. This means that all Personal Data about the individual who has withdrawn the consent must be deleted or anonymized, including Personal Data in any backups.

### *Additional requirements for Processing Special Categories of Personal Data*

Special Categories of Personal Data, often called “Sensitive Personal Data”, are afforded special protection and should not be Processed by Getinge except under special circumstances.

Processing of Special Categories of Personal Data may only be performed if there is a legal basis for the Processing as described above in this Section 6. In addition, such data may only be Processed if at least one of the following conditions are met:

a) The Data Subject has provided explicit consent to the Processing for the specified purpose(s);
b) The Processing is necessary for the purposes of carrying out the obligations and exercising rights of the Data Controller or the Data Subject in the field of employment law in so far as authorized by national laws or collective agreements;
c) The Processing is necessary for the establishment, exercise or defense of a legal claim; or
d) The Processing is necessary for the purpose of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health care or treatment.

Getinge should generally avoid Processing Special Categories of Personal Data, and may only do so if one or more of the above applies. Local exceptions may also apply.

**NOTE!**

Explicit consent contains the requirements of a regular consent as described above in this Section 6 regarding consent and withdrawl of consent. In addition, the individual shall be clearly presented with an option to agree or disagree with the proposed Processing of Personal Data.

### *Personal Data in the scope of criminal offences and convictions*

Getinge shall not Process any Personal Data relating to criminal offences or convictions, including suspicions, except when permitted or required by applicable laws and regulations. Note that there is a general prohibition to Process this type of Personal Data. However, exemptions may be found in national laws and regulations.

There may be requirements on different Getinge departments to Process Personal Data relating to criminal offences, convictions or related suspicion. For example, in the context of investigations and/or due diligence there are requirements (where supported by applicable law and regulation) on the Legal, Compliance & Governance department to perform fact finding, background checks on companies and/or personnel in relevant positions.

**NOTE!**

The Data Privacy Team shall always be consulted before Processing any Personal Data concerning criminal records, criminal offences, convictions or related suspicions.

## Information to Data Subjects

Getinge shall give Data Subjects written notice with information on:

a) The name and contact details of the entity who is the Data Controller;
b) The types of Personal Data Processed and the related purposes of the Processing;
c) The legal basis of the Processing;

d) How long Personal Data will be kept;
e) The recipients or categories of recipients of the Personal Data;
f) Information on the Data Subject's rights in accordance with Section 8 below; and
g) If applicable:
    i. contact details to the responsible Data Protection Officer;
    ii. from where Personal Data has been obtained;
    iii. the consequences if a Data Subject does not provide his/her Personal Data;
    iv. Getinge's intentions to transfer Personal Data outside the EU/EEA in accordance with Section 9 below; and
    v. Information about profiling.

The Data Privacy Team provides template privacy notices that shall always be used when a Getinge company needs to inform Data Subjects about Processing of Personal Data. The templates contain further instructions on the information that must be provided to Data Subjects.

It is the responsibility of each Getinge company to ensure and demonstrate that its privacy notices are sufficient and complete and that it complies with Data Protection Laws. In addition, Getinge companies shall translate privacy notice(s) into local language if necessary.

In relation to employees, information about Processing of Personal Data is usually provided in the Employee Privacy Notice which the employees' receive together with the employment contract. Each Getinge company shall ensure that its Employee Privacy Notice is easily accessible to the employees and up to date as well as provides sufficient information about how the company Processes Personal Data about employees.

## Changed purposes for Processing of Personal Data

Before changing the purposes for Processing of Personal Data, a Getinge company shall:

a) Assess the legality of the Processing of Personal Data and document the assessment in accordance with Section 7 below;
b) Provide the Data Subject with written information describing the amendments to the purposes of the Processing; and
c) If the Processing is based on consent, obtain a new consent from the Data Subject.

## Profiling and automated decision-making

### *General about profiling*

Profiling entails any form of automated Processing of Personal Data involving the intention to evaluate personal aspects relating to a Data Subject or predict or analyze that Data Subject's performance at work, economic situation, location, health, personal preferences, interests, reliability or behavior, driver behavior, customer behavior, location or movement.

Profiling is often used to make predictions about individuals by using data from various sources and make statistical deductions. The purpose of the Processing could be to analyze the Data Subject's characteristics or behavior patterns in order to place them into a certain group or category. This enables the Data Controller to make predictions about for example the Data Subject's interests, ability to perform a task or likely behavior.

**EXAMPLES**

Profiling may for example consist of analyzing an individual's behavior on websites through cookie identifiers or IP-addresses in order to send personalized advertisement concerning specific products or services. Another example of profiling concerns analysis of previous purchases in order to predict future purchases. Therefore, profiling is a method commonly used in connection with direct marketing and social media, but could also be used for other Processing activities such as in research studies.

### *Decisions based on profiling*

A decision made by a Getinge company based on profiling, shall only be allowed when:

a) it is absolutely necessary for entering into, or for the performance of, an agreement between the Data Subject and the Data Controller (this exception should be interpreted narrowly);
b) it is expressly authorised by law, including for fraud and tax evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of institutions or national oversight bodies, and to ensure the security and reliability of a service provided by Getinge; or
c) the Data Subject has provided explicit consent.

### *Requirements*

Getinge companies shall ensure the following when engaging in profiling:

a) Only Process necessary Personal Data to fulfill the purpose;
b) Provide Data Subjects with sufficient information about the profiling in accordance with Section 6. If the profiling concerns automated decision-making, the Data Subjects has a right to obtain an explanation about the reached decision as well as information about the right to object to such decision;
c) Use adequate mathematical or statistical procedures for the profiling;
d) Implement appropriate technical and organizational measures in accordance with Section 0; and
e) Secure Personal Data in a way which takes into account the potential risks involved for the rights and interests of the Data Subjects and which, inter alia, prevents discriminatory effects against individuals on the basis of Special Categories of Personal Data or that result in measures having such effect.

**NOTE!**

Profiling shall be pre-approved by the Data Privacy Team before it is conducted.

## Data retention, storage and deletion of Personal Data

Getinge companies shall ensure Personal Data is not Processed longer than:

a) necessary in relation to the purpose(s) of the Processing; and
b) permitted by Data Protection Laws.

Getinge companies shall implement processed to ensure the requirements in this Section are fulfilled.

**NOTE!**

Some countries (e.g. Russia and China) require that all Personal Data about its citizens are stored within the county's borders. In other countries, there may be requirements to store specific Personal Data locally if it is Processed for specific purposes (e.g. Sweden requires accounting information to be stored within its borders). The localization requirements do normally not prevent Getinge from also storing a copy of the Personal Data elsewhere, if such storage is necessary.

# 7. Assessment and documentation of Processing

## Record of Processing activities

When required by Data Protection Laws, Getinge companies are responsible for keeping a record of the companies' Processing activities. All records shall be maintained in the compliance tool chosen and handled by the Data Privacy Team. Further information can be found on the Data Privacy Intranet page.

The requirements in this Section applies both when Getinge companies are acting as Data Controllers and Data Processors.

## Assessment of legality before initiating a new Processing activity

Before conducting a new Processing activity or making changes to an ongoing activity, Getinge companies shall assess the legality of the Processing of Personal Data and document the assessment. This also applies to any ongoing Processing activities that have previously not been assessed and/or documented.

The requirements in this Section applies both when Getinge companies are acting as Data Controllers and Data Processors.

## Data Protection Impact Assessments

If Processing of Personal Data is likely to result in a high risk to the rights and freedoms of Data Subjects, Getinge companies shall, before such envisaged Processing is initiated, perform an assessment of the impact of the Processing operations on the protection of Personal Data (Data Protection Impact Assessment). A Data Protection Impact Assessment may in particular be of relevance when Getinge companies uses new technologies and taking into account the nature, scope, context and purposes of the Processing.

Data Protection Impact Assessments shall always be performed by the Data Privacy Team on behalf of a Getinge company. The Getinge company shall cooperate with the Data Privacy Team during the course of the assessment, including but not limited to providing necessary information.

# 8. Data Subject rights

## Handling of Data Subject requests

The following applies regarding requests from Data Subjects:

a) All requests from Data Subjects shall be forwarded immediately to and handled by the Data Privacy Team.
b) Data Subjects may not face negative consequences when exercising Data Subjects rights.
c) All Data Subject requests shall be handled with confidentiality.
d) Getinge companies shall cooperate with the Data Privacy Team in order for the Data Privacy Team to be able to answer requests in a timely manner.

Note that Data Subject rights are not absolute and that exceptions may apply.

## Processes to handle Data Subject rights

Getinge companies are responsible for implementing processes to assist the Data Privacy Team with handling of Data Subjects' rights to:

a) Request access to Personal Data. This includes the Data Subjects' right to receive information about the Processing of Personal Data relating to the individual in question and ensuring the right to data portability.
b) Request correction of inaccurate Personal Data.
c) Request erasure of Personal Data.
d) Object at any time to Processing of Personal Data when the Processing is based on Getinge's legitimate interest, including when the Processing concerns profiling.
e) Obtain restriction of Personal Data.

# 9. Transfers of Personal Data

## General about transfers

Personal Data shall only be transferred to fulfill the purpose(s) of the Processing. Transfers of Personal Data does not only include sending Personal Data by the use of electronic messages such as by e-mail, but also include when Personal Data can be accessed or viewed. Personal Data is considered as transferred even if it is only temporarily accessed, viewed or otherwise Processed.

**EXAMPLE**

Personal Data is transferred when a Getinge company in France stores Personal Data in a folder, which can be accessed by Getinge employees in China (see also in this Section 9 regarding transferring Personal Data from the EU/EEA to a country outside the EU/EEA).

## Transferring Personal Data from the EU/EEA to a country outside the EU/EEA

As a main rule, Getinge companies in the EU/EEA shall not transfer Personal Data outside the EU/EEA. Such transfers may only be made if strictly necessary.

If transfers of Personal Data from countries in the EU/EEA to countries outside the EU/EEA are strictly necessary, Getinge companies shall ensure that:

a) such transfers are subject to adequate safeguards in accordance with Data Protection Laws, including but not limited to transfers based on:
   i. An adequacy decision made by the European Commission;
   ii. The EU Standard Contractual Clauses adopted by the European Commission; or
   iii. Explicit consent.
b) a Transfer Impact Assessment has been made if necessary.

Prior to a transfer of Personal Data, Data Subjects have the right to receive information about the transfer and the applicable adequate safeguard in accordance with Section 6.

# 10. Sharing and disclosing Personal Data within Getinge

Getinge employees and consultants shall only share and disclose Personal Data to individuals within Getinge who need such data for performance of work tasks and where there is a legitimate business purpose for sharing or disclosing such Personal Data. Personal Data may only be shared or disclosed to the extent necessary in order to fulfill the purpose(s) of the Processing. Personal Data may not be shared or disclosed because it may be “nice to have” for the recipient.

# 11. Data Processors

## General about clauses in agreements

It is the responsibility of Getinge companies to, if necessary, include Personal Data Processing clauses and/or data processing agreements in Getinge’s standard business and employment agreements.

In cases when existing agreements are already in place, Getinge companies shall update such agreements when necessary with Personal Data Processing clauses and/or relating data processing agreements.

**NOTE!**

The data processing agreement templates available on the Data Privacy Intranet page should always be used in cases when a data processing agreement is required.

## Getinge as Data Processor in relation to third parties

If a Getinge company Processes Personal Data on behalf of a third party (such as a customer), Getinge and the third party shall enter into a data processing agreement. The Getinge company shall ensure that the applicable template available on the Intranet is used.

**EXAMPLE**

Getinge is in most cases acting as Data Processor in connection with provision of our software solutions to hospitals. This is the case when Getinge needs to access or otherwise Process Personal Data when we provide software support. For these situations, the hospital will act as Data Controller.

### Contracting an external Data Processor

If a third party will Process Personal Data on behalf of Getinge (such as a supplier), Getinge and the third party shall enter into a data processing agreement. The Getinge company shall ensure that the applicable template available on the Intranet is used.

**EXAMPLE**

If Getinge purchases a new IT system/solution which includes that the supplier of the IT system/solution Processes Personal Data on behalf of Getinge (such as storing Personal Data and/or accessing Personal Data when providing support), Getinge and the supplier shall enter into a data processing agreement. In this situation, Getinge is the Data Controller and the supplier is the Data Processor.

### Getinge as Data Processor in relation to other Getinge companies

If a Getinge company Processes Personal Data on behalf of another Getinge company, the parties shall enter into an intra-group data processing agreement. The Getinge companies/functions shall ensure that:

a) the applicable template available on the Data Privacy Intranet page is used; or
b) an intra-group data processing agreement has already been entered into.

**EXAMPLE**

If Getinge IT assists Getinge HR with support which includes that Getinge IT Processes Personal Data on behalf of Getinge HR, an intra-group data processing agreement shall to be entered into. In this case, Getinge IT is the Data Processor and Getinge HR is the Data Controller.

## 12. Technical and organizational security measures

All Getinge companies shall comply with Getinge's policies and directives regarding information security. Getinge companies shall also implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The following should be taken into account when such measures are implemented:

a) The state of the art;
b) The cost of implementation;
c) The nature, scope and purposes of the Processing; and
d) The risk of likelihood and severity for the rights and freedoms of Data Subjects.

It is the responsibility of each Getinge company to ensure that Processing of Personal Data complies with Data Protection Laws, including taking appropriate technical and organizational measures such as access rights, flagging Personal Data for deletion, automated deletion and logging data. With regards to access rights, Getinge companies shall ensure that access to Personal Data reflects the roles of employees and consultants, including in cases of changed roles within Getinge.

# 13. IT solutions Processing Personal Data

It is the responsibility of each Getinge company to ensure that new and existing IT functions, solutions and/or services used to Process Personal Data comply with Data Protection Laws, including but not limited to requirements regarding:

a) Privacy by design and by default;
b) Data retention;
c) Data Subject requests, including data portability;
d) Sufficient technical and organizational security measures; and
e) Access rights.

Before a new IT solution is used and before changes are made to an existing IT solution, Getinge companies shall in a timely manner inform the Data Privacy Team of privacy risks, purposes and the Personal Data being Processed. Information shall also be provided to the Data Privacy Team about Processing of Personal Data in existing IT solutions.

*See further: Information Security Directive*

# 14. Privacy by design and by default

The principles of privacy by design and by default should be taken into account when Getinge is developing, designing, selecting and using applications, services and products that include Processing of Personal Pata. These principles should be implemented both at the time of the determination of the means for Processing and at the time of the Processing itself.

Privacy by design is a concept and approach to system engineering that takes data protection into account throughout the engineering process. Privacy by design focuses on ensuring that privacy is embedded into information technology, business processes, physical spaces and networked infrastructures from the outset.

Getinge should ensure that their systems and processes are especially designed with data protection in mind. Data protection should not be an afterthought, but built into the fabric of how the entity conducts its business.

Privacy by default means that the Data Controller shall implement mechanisms for ensuring that, by default, only necessary Personal Data is Processed for each specific purpose of the Processing and is especially not collected or retained beyond what is necessary for those purposes, both in terms of the amount of data and the time of storage. In particular, implemented mechanisms shall ensure that Personal Data by default is not made accessible to an indefinite number of individuals.

**EXAMPLE**

As an example, it would be relevant to consider privacy by design and by default when Getinge builds new IT systems for storing or accessing Personal Data, develops policies or strategies that have data privacy implications, initiates Personal Data sharing or usage for new purposes.

Designing projects, processes, products or systems with privacy by design and by default in mind at the outset has several benefits, including:

a) The possibility to identify potential problems at an early stage where addressing them often is simpler and less costly;
b) The awareness of data privacy across the organization is increased;
c) The likeliness to meet the obligations of Data Protection Laws increases and equally, the likelihood of breaches is decreased; and
d) Projects, processes, products or systems are less likely to be privacy intrusive and have a negative impact on individuals.

Especially when Getinge designs and develops products and services relating to Personal Data, the relevant details on how Getinge should comply with the privacy by design and by default requirements should be defined.

## 15. Personal Data Breaches

All Personal Data Breaches shall immediately be reported in accordance with the process described on the Data Privacy Intranet page.

Getinge companies shall:

a) ensure all solutions used for Processing of Personal Data enable reporting of Personal Data Breaches;
b) implement measures supporting detection of Personal Data Breaches;
c) document the circumstances of a Personal Data Breach, including effects, possible risks and taken or planned remedies; and
d) cooperate with the Data Privacy Team when Personal Data Breaches are investigated and remedied.

*See further: Personal Data Breach Directive*

## 16. Supervisory Authorities

All contacts with Supervisory Authorities shall be handled by the Data Privacy Team. Getinge companies shall cooperate with the Supervisory Authorities upon request.

## 17. Deviations

Deviations from this Global Policy shall be approved on the same level of authority as when the Global Policy was originally approved.

## 18. Breaches against the Global Policy – Speak Up

Do not hesitate to raise a concern. Any Getinge employee who suspects violations of this Global Policy is expected to speak up and raise the issue to their line manager, to the Ethics and Compliance Office, or to use the Getinge Speak Up Line. The Getinge Speak Up Line is available on Getinge internal and external webpages. At Getinge we do not accept any form of retaliation against someone who speaks up, expressing concerns or opinions.

*See further: Global Speak Up and Non Retaliation Directive*

## 19. Roles and responsibilities

All Getinge employees are individually responsible for reading, understanding and complying with this Global Policy. Each employee is responsible for acting in accordance with this Global Policy.

Every line manager is responsible for making sure each team member has access to this Global Policy and related Directives, Instructions and Guidelines.

Day-to-day reinforcement, including regular information and training in the area of data privacy, as well as compliance follow-up, is part of every manager's responsibility.

Violations against this Global Policy can lead to disciplinary action, up to and including termination.

## 20. Guidance and assistance

To guide our conduct when it comes to Getinge's standpoints in the area of data privacy, there is this Global Policy and several directives, and instructions. If you have questions on this Global Policy or you are uncertain which rules apply, please contact the Data Privacy Team.

## 21. Useful links

| **Title** |
| --- |
| Personal Data Breach Directive |
| Data Privacy Governance Directive |
| Information Security Directive |
| Global Speak Up and Non-Retaliation Directive |