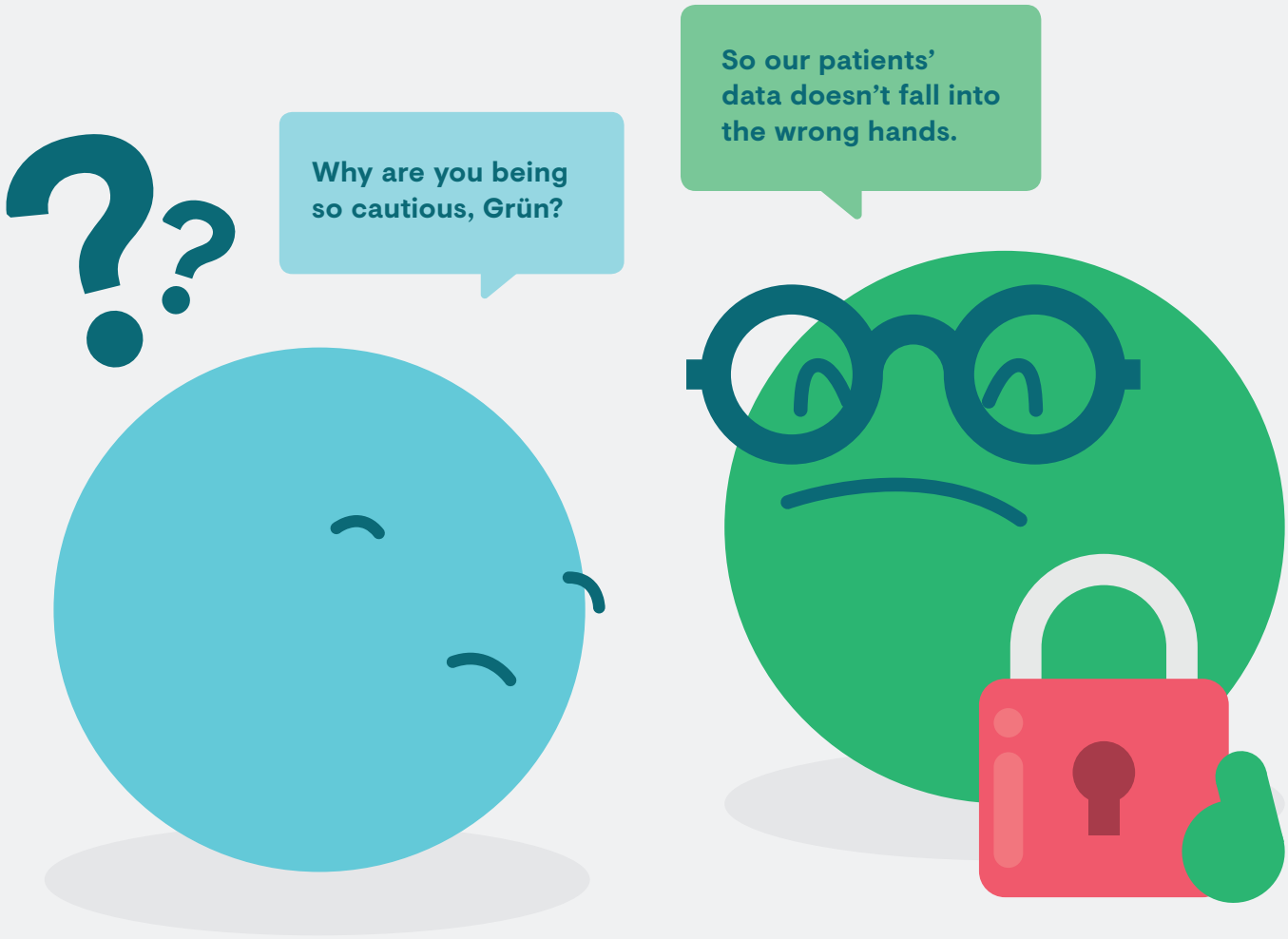
Data Protection Policy



Maximise business.
Minimise risk.

GRÜNENTHAL

All Grünenthal employees have to respect data protection standards and applicable laws and regulations in their business activities to protect Grünenthal from exposure to potential personal data breaches.

Who is concerned?

This Policy applies to all Grünenthal employees in legal entities belonging to the Grünenthal Group (in particular, but not limited to Grünenthal Pharma GmbH & Co. KG and Grünenthal GmbH) who are involved in the processing of personal data in the European Union.

This Policy also applies to all Grünenthal entities outside the European Union processing personal data of data subjects who are in the European Union where and as far as the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the European Union; or
- the monitoring of data subjects´ behaviour as far as their behaviour takes place within the European Union.

All non-German Grünenthal entities in scope of this Policy have to implement the provisions of this Policy in a local Policy also considering additional requirements deriving from local legislation on the topic of the processing of personal data.

All Grünenthal employees have to respect data protection standards.

How to use this Policy

This Policy has to be applied in conformity with national laws and regulations. If national laws and regulations are stricter than the rules set out in this Policy they have priority. If national law provides the basis for explicit exceptions from the rules set out in this Policy, make sure with Local Compliance that your actions are covered by these exceptions. Please check with Local Compliance if there are national supplements to this Policy that you have to take into account, too.

What is concerned?

We are responsible for ensuring the correct handling of personal data by Grünenthal and any third party engaged to act on Grünenthal's behalf. Accordingly, all Grünenthal employees contracting third parties must verify and ensure the correct handling of personal data by those third parties.

This Policy defines processes and responsibilities for Grünenthal's data protection standards. There are four major data subject groups on which we handle personal data at Grünenthal:

- Employee data (e.g. data on job applicants, active and former employees).
- Patient and volunteers data (e.g. data collected during clinical research, adverse event reporting or handling of medical enquiries).
- Customer and supplier data, as well as data from third parties collaborating with Grünenthal (e.g. healthcare professionals, partners, consultants).
- Data from any other individual outside the three groups mentioned above (e.g. relatives of employees).

The application of this Policy for specific cases may be further detailed in supportive documents (position papers; SOPs etc.).

What is data protection?

Data protection is the act of ensuring that:

- all processing activities by Grünenthal are lawful and compliant with the requirements of all applicable data protection laws and regulations.
- the collection and use of personal data is limited to the minimum necessary.
- natural persons whose data are processed are clearly informed in a transparent way on how, why, by whom, for which purpose and for how long their data is collected and used.
- personal data is processed on a lawful basis, e.g. natural persons whose data are processed have given their informed consent to the processing of their personal data.

Data privacy is a synonym in non-EU countries for data protection, used in European guidelines and laws.

This Policy covers the following topics:

Responsibilities

The roles and responsibilities listed in this Policy are as follows:

Role	Responsibility
Data Protection Coordinator	**Data protection contact within the local/global Grünenthal department or affiliate, who within his/her organisation or function:** • Provides guidance to employees on how to follow our ● Data Protection Policy • Answers questions and issues related to data protection • Informs Global/local Compliance if any issue is identified or corrective action required • Proactively identifies data protection needs in new projects and systems • Identifies any changes in data protection regulations applicable • Supports the implementation of controls and data security measures.
Local Data Protection Officer (DPO) *(as required by Art. 37 GDPR and the German Federal Data Protection Act 2018)*	• Data Protection Officer designated according to Art. 37 GDPR, local data protection laws or on a voluntary basis • Contact person and expert for questions related to data protection, especially for the employees • Creates transparency regarding the operational data processing (i.e. training of our employees, performing data protection assessments; prior checking of new procedures) • Secures compliance with all relevant applicable data protection laws • Supports the further enhancement of our data protection program
Global Data Protection Officer (Global DPO)	• Oversees local and global activities related to the implementation of and adherence to our data protection program and other privacy policies, procedures and standards in coordination with Local DPOs and DPC • Supports Local DPOs and DPCs with expert knowledge on international and local data protection rules • Takes privacy relevant decisions on a global level and supports Local DPOs and DPCs in finding adequate solutions for local implementations • Develops data protection trainings for all functions and oversees and supports local training activities by Local DPOs and DPCs
Global/Local Compliance	Supports global/local implementation of this Policy.
Legal Department (Global Legal)	Performs legal review of data protection related topics and provides legal advice in addition to the support from the DPO.
Senior Management	Supports and ensures implementation of this Policy, training and adequate monitoring in their department or affiliate.

Definitions and abbreviations

Definitions and abbreviations of terms used in this Policy are explained here:

Role	Responsibility
Consent	Freely given, specific informed and unambiguous permission received from a natural person on the processing of his/her personal data.
Data Controller	A natural or legal person, public authority, agency or any other body which determines the purposes and means for which and the way any personal data are or are to be processed.
Data Processing	Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as the collection, storage, retention, adaptation, modification, reading, retrieval, use, transmission by data transfer, blocking, erasure disposal or disclosure by transmission, dissemination or other means. This also includes carrying out the inspection or maintenance of automated procedures or data processing systems, in the course of which the possibility of personal data being accessed cannot be excluded.
Data Transfer	The disclosure, transmission or process of making personal data available between Grünenthal entities and between Grünenthal and third parties.
Data Subject	Each identified or identifiable, directly or indirectly, natural person whose data is processed.
External Data Processor	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
GDPR	General Data Protection Regulation of the European Union.
Personal Data	Any information about an identified or identifiable natural person regardless of the format in which it is displayed (hardcopy or digital). With this kind of data, a living individual can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data processor. The individual may be identified by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special categories of Personal Data *(according to Article 9 GDPR)*	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data to uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

1. Collection of personal data

Collection of personal data is only permitted, if either:

- the collection of personal data is explicitly permitted by applicable (data protection) laws such as the GDPR (e.g. processing is necessary for the performance of a contract with the data subject, compliance with legal obligations, the protection of vital interests, the performance of a task carried out in the public interest or for the purposes of the legitimate interests pursued by the controller or by a third party) or
- the natural person whose data is processed has provided his or her explicit, unambiguous, informed and freely given consent.

1.1 Direct collection of personal data

Generally, personal data must be collected directly from the natural person whose data is processed. In such cases we have to fulfil our information duties according to Article 13 GDPR. The data subject must be provided with the following information:

- identity and contact details of the controller (Grünenthal, local entity or affiliate).
- contact details of the data protection officer (Local DPO), if designated.
- the purpose of the processing and the legal basis for the processing.
- if applicable, the legitimate interests pursued by the controller.
- if applicable, the recipients or categories of recipients of the personal data.
- if applicable, the intention to transfer the personal data to a third country outside the EU and the existence or absence of appropriate safeguards.
- the retention period or, if that is not possible, the criteria used to determine that period.
- the existence of rights regarding access, rectification, erasure or restriction of processing of personal data as well as the right to data portability.
- if applicable, the right to withdraw consent at any time.
- the right to lodge a complaint with the supervisory authority.
- whether the provision of personal data is a statutory or contractual requirement, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.
- if applicable, the existence of automated decision-making, including profiling and, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

1.2 Indirect collection of personal data

Personal data may be collected from other sources or without the data subject noticing it only in cases where applicable law permits it or in cases in which the data subject has provided his or her valid consent prior to the collection of personal data.

If personal data is collected not directly from the natural person whose data is processed, we have to notify him/her about the data that we have to fulfil our information duties according to Article 14 GDPR.

The data subject must be provided with the following information:

- all above mentioned information as required for the direct collection of personal data (see above chapter 1.1).
- from which source the personal data originates, and if applicable, whether it came from a publicly accessible source.
- the categories of personal data concerned.

1.3 Consent requirements

In case consent is used as basis for collection and processing of personal data, consent must be:

- unambiguous.
- freely given.
- detailed or “informed”, as a minimum it should contain:
  - name and address of the data controller (Grünenthal legal entity).
  - purpose of collection, processing or use.
  - type of personal data to be collected (e.g. general data, consumer behaviour, DNA and genetic information, etc.).
  - clarification of whether consent shall be the basis for processing special categories of personal data. If yes, the consent must explicitly refer to such data.
  - categories of recipients (processors) who will receive or access the data.
  - transfers of personal data to third countries or international organisations, if applicable and information on the existing safeguards to ensure an adequate level of data protection.
  - the information that the data subject may withdraw his or her consent at any time.

This consent can be collected as follows:

- in writing.
- electronically or digitally.
- verbally or by any other affirmative action that clearly indicates the wish of the natural person whose data is processed.

  (Since a verbal consent or other affirmative action is hard to prove, those forms of consent should only be used in exceptional cases, e.g. adverse event reporting via phone; in such cases it is important to at least create a telephone note with the date of the call, the brief content of the consent and the name of the employee that took down the note.)

The consent can be withdrawn by the data subject at any time and without difficulties. The data subject is to be informed about that prior to giving consent.

Employees must proactively contact their Data Protection Coordinator or DPO/Local or Global Compliance before collecting personal data in a new activity to secure that the proposed consent fits all legal requirements.

1.4 Special categories of personal data

Special Categories of personal data **must not** be collected, unless:

- the data subject gives his/her valid consent, or
- the personal data concerned relates to data which are manifestly made public by the data subjects themselves, or
- there is an existing legal requirement or permission to collect the data concerned.

When Special Categories of personal data have to be processed, the responsible Grünenthal employee must liaise with the responsible Data Protection Coordinator (or Local DPO) and/or Global/Local Compliance to conduct an evaluation of the necessity of data and the adequate level of protection.

“The consent can be withdrawn by the data subject at any time and without difficulties.”

2. Processing of personal data

Employees must adhere to the following principles when processing any sort of personal data.

Principle of purpose limitation:

- Employees have to define specific purposes for which the personal data shall be used prior to collecting the personal data.
- In case consent is used as basis for processing of personal data, employees must ensure that they collect consent in a way that all prior defined purposes are covered by the text of the consent.
- Personal data must be processed and used only for the purposes for which they were collected; Personal data must be kept only as long as it is necessary to satisfy the purposes for which the data was collected and stored. They must be disposed of respecting the specific defined timelines for retention of personal data. Storing personal data for longer than necessary for the intended purpose requires additional explicit consent of the data subject, if not required or permitted by law.
- Personal data that were collected for different purposes must not be combined or cross-referenced.
- Generally, change of purpose is not allowed. If personal data stored in our systems shall be used for other purposes than the initial purposes, employees are required to notify the DPO hereof, prior to processing the personal data for the new purposes.

Principle of data minimisation/ privacy by design:

- Employees have to ensure, that they only collect the personal data that are strictly necessary to fulfil the specified purpose(s). They shall plan processing activities with the possibility of anonymisation and pseudonymisation in mind and make use of such techniques wherever possible to avoid the processing of personal data whenever possible.
- Whenever more data is collected than necessary for the specified purposes, you will always have to obtain the valid consent of the data subject for such “additional data”.

Principle of transparency:

- Grünenthal has to be transparent about the purposes of the data as well as the major aspects of the processing itself.
- Data subjects can contact anyone within Grünenthal to be informed about his/her personal data actually held by Grünenthal.
- Any external request from a data subject to provide access to the personal data Grünenthal possesses about him/her must be submitted **immediately** to Global Compliance and/or to our Global Compliance and/ or to our Local DPO/DPC for follow-up.
- Any request from an employee on his/ her personal data held by Grünenthal must be submitted to and provided by the employee’s HR contact person, who then will take care about the information provision.
- Information about personal data must be provided to the data subject in a clear and plain language within a period of just one month as provided in the GDPR. In exceptional cases, this period may be extended by two further months.
- If you are uncertain, whether a data subject is requesting access to his/her personal data, immediately contact the DPO to clarify the situation.

3. Data transfers and data disclosure

If personal data is transferred between Grünenthal entities or to other third parties, employees must ensure that:

- Global Compliance and/or the Local DPO/DPC has been contacted to verify the admissibility of such transmission (e.g. if personal data will be transmitted to states outside the EU/EEA).
- the disclosure or transfer of personal data is:
  - required for any legal purpose (e.g. court case).
  - covered by unambiguous consent.
- standard data protection annex, developed by HQ or locally, is included in any agreement with external and internal data processors.

Data disclosure between departments within one legal entity is permitted only insofar that this is necessary for the receiving department to accomplish its tasks.

4.
Data security

“Personal data must be handled in a way that its confidentiality, integrity and availability is ensured.”

Data Protection Policy

Departments involved in the processing of data in any way, must implement the technical and organisational measures required to guarantee compliance with the provisions of the data protection regulation. Details regarding the necessary technical and organisational measures are set out in specific Grünenthal guidelines (please contact it-security@grunenthal.com for more details).

Personal data must be handled in a way that its confidentiality, integrity and availability is ensured and that access to the data is limited to a minimum of people and systems (“need-to-know principle”).

Personal data must be protected against unintended or unlawful erasure, alteration or loss as well against unauthorised disclosure or access. Especially, personal data in digital form (servers and workstations), networks or communication links and applications have to be protected in a reasonable way (with suitable techniques and acceptable costs).

Any new IT system (on premises or externally provided like cloud services) used by Grünenthal needs to be reviewed by Global IT with respect to the respective Grünenthal guidelines to fulfil data protection and other data security obligations (please refer to IT Demand Management Guideline).

5. Rights of the data subjects

Right to access (Article 15 GDPR)

The data subject has the right to obtain confirmation as to whether or not personal data concerning him/her are being processed, and where this is the case, access to the personal data.

Right to rectification (Article 16 GDPR)

The data subject has the right to obtain the rectification of inaccurate personal data concerning him/her and to have incomplete personal data completed (e.g. by providing a supplementary statement).

Right to erasure/“right to be forgotten” (Article 17 GDPR)

The data subject has the right to demand that personal data concerning him/her is erased if the processor is not or no longer authorised to keep the personal data (e.g. the data is no longer necessary, the data subject has withdrawn consent or the data has been unlawfully processed).

Keep in mind, that not all data has to be erased and that some data might be retained due to a legal obligation.

Right to restriction of processing (Article 18 GDPR)

The data subject has the right to obtain a restriction of processing if, for example, the accuracy of the data is contested, the processing is unlawful, or the data is no longer needed for the original purposes but is retained for the exercise or defence of legal claims.

Right to data portability (Article 20 GDPR)

The data subject has the right to receive the personal data concerning him/her, which he/she has provided to a controller, in a structured, commonly used and machine-readable format. Where technically feasible, he/she has the right to have the personal data transmitted directly to another controller without hindrance.

Right to object (Article 21 GDPR)

The data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6 (1) GDPR, including profiling based on those provisions. In such case, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

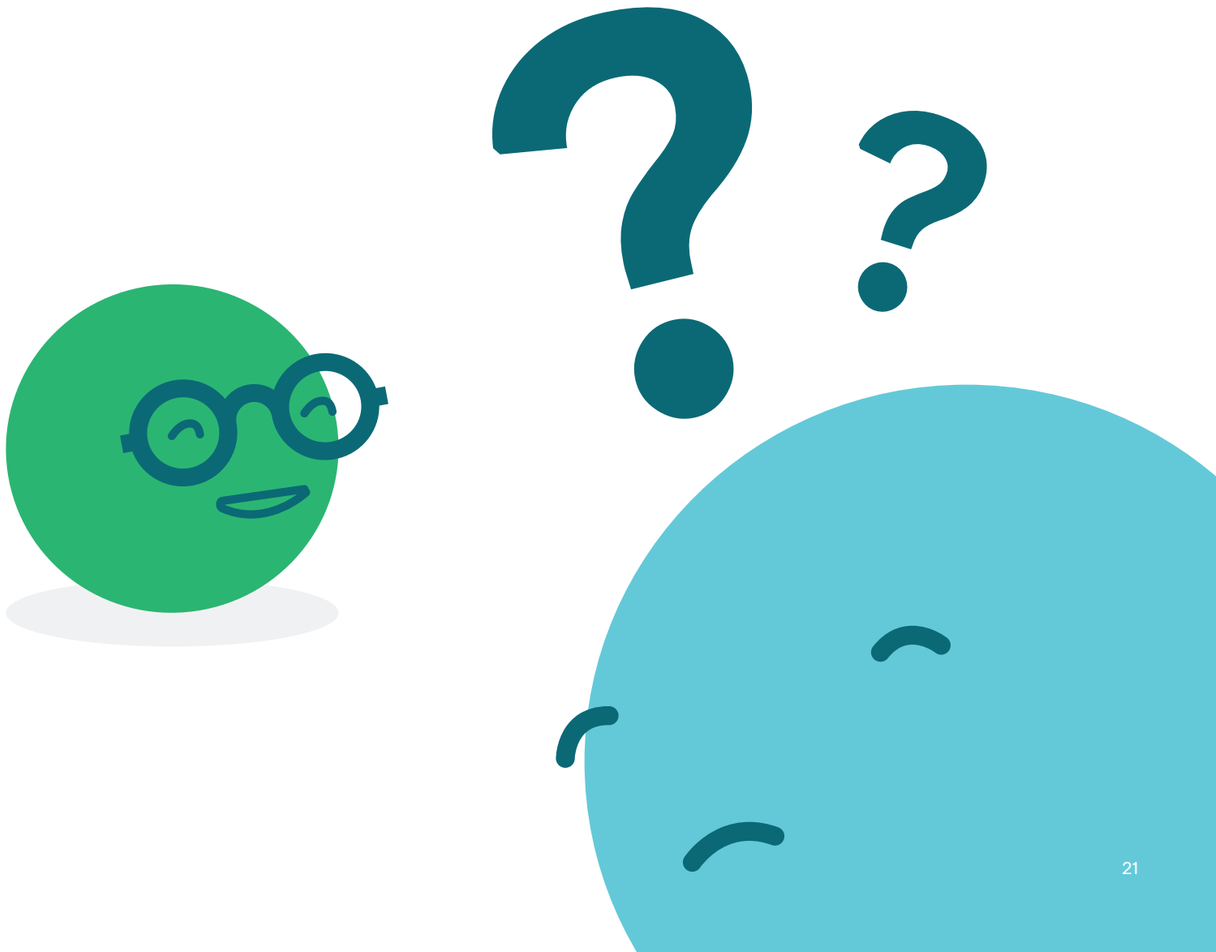
6. Data protection officer

Each Grünenthal entity based in an EU member state must appoint a Data Protection Officer (Local DPO) if the following requirements are fulfilled:

- the core activities of the entity consist of processing on a large scale of Special Categories of personal data (e.g. health data), or
- the core activities of the entity consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- any other provisions in the GDPR or local legislation require the mandatory appointment of a Local DPO.

Employees must involve the Local DPO regarding:

- the development or changing of data processing procedures which include personal data.
- any violation of the data protection provisions as described in this Policy.
- any inspection or audit planned with respect to data protection including inspections of third parties acting on behalf of Grünenthal (e.g. contractors) if the inspection affects personal data collected for Grünenthal.



7. Records of processing activities

> **“ Records of processing activities are required for companies processing personal data. ”**

Records of processing activities are required for companies processing personal data. They provide an overview of the data processing procedures in use.

The inventory has to provide an overview about the processing of personal data, electronic systems and paper files where personal data are managed. In addition, the purpose, legal basis, data types, recipients, retention periods, technical and organisational measures and data processors are to be documented.

Therefore, the process owner must notify the Local DPO/DPC and Global Compliance in due time before new procedures or systems are introduced or, if already existing procedures are changed, such procedures can be incorporated into the records of processing activities. Oftentimes, it is crucial to inform the Local DPO/DPC in an early stage of the planning phase. He/she will help to identify data protections risks and may provide helpful advice on how to design a data processing activity.

The process owner must perform a regular review of existing procedures (e.g. annually or bi-annually) to ensure that they are accurate, updated and supervised by the Local DPO/DPC.

If processing activities are likely to result in a high-risk to the rights and freedoms of natural persons, the process owner must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (Data Protection Impact Assessment). The determination whether such high-risk is given and the assessment itself will be supported by the Local DPO/DPC.

8. Management of data breaches

“The Local DPO/DPC will evaluate whether an incident must be reported to the responsible Data Protection Authority and/or the affected individuals.”

In each case where a breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by Grünenthal or one of its processors, this must be reported to the Local DPO/DPC immediately.

The report to the DPO/DPC must contain of all relevant information helping to evaluate the facts, in particular:

- Detailed description of the incident and on which categories of personal data are involved (“What?”).
- The time the incident occurred (“When?”).
- The location and systems or processing activities affected (“Where?”).
- The acting employees and third parties involved in the incident (“Who?”).
- The counter measures that have already been taken to prevent a negative impact on the rights of the data subjects.

The Local DPO/DPC will evaluate whether an incident must be reported to the responsible Data Protection Authority and/or the affected individuals. Only the Local DPO/DPC in coordination with the Global DPO will communicate with the Data Protection Authorities.

What?/When?/Where?/Who?

9. Additional requirements for German entities

10.1 Appointment of a Data Protection Officer

German Grünenthal entities must appoint a Local DPO if:

- they constantly employ as a rule at least ten persons dealing with the automated processing of personal data.
- they undertake processing operations subject to a data protection impact assessment pursuant to chapter 7.
- they commercially process personal data for the purpose of transfer, of anonymised transfer or for purposes of market or opinion research.

10.2 Special requirements for the processing of employee data

Internal investigations

Any measures taken to detect crimes committed by employees may only be conducted if there is a documented reason to believe the data subject has committed a crime while employed and the processing of the employee´s personal data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason. Any such activity must be aligned with the responsible Local DPO/DPC upfront.

Special categories of personal data

In addition to what is outlined in chapter 1.4, special categories of personal data of an employee may also be processed for employment-related purposes if it is necessary to exercise rights or comply with legal obligations derived from labour law, social security and social protection law, and there is no reason to believe that the data subject has an overriding legitimate interest in not processing the data.

Any questions?

You may contact our Data Protection Team and your Local Data Protection Officer at any time using the contact details published on the intranet.

compliance@grunenthal.com

Grünenthal GmbH, 52099
Aachen, Germany