



Number:

Title:

Title (EN):

Type:

Scope:

Area:

Country:

Previous Number:

Document Information

Revision:

Status:

Effective Date:

	Standard Operating Procedure Grünenthal, 2345 Brunn/Geb., Austria			
document no.	replaces document no.	from	page	of
AT-GE-577-0002-01	-/-	-/-	1	10
valid from	01 DEC 2017	attachments	-/-	
Data Protection at Grünenthal G m.b.H Austria				

SDN05-GL-QA-102-A001-01

Regulatory area(s) GCP GLP GMP GVP

Other area(s) All

Language version Original Translation

Prepared by Dr. Marion Kubista-Andersson
Head of Medical, Reg. Affairs
and Quality Assurance
Local Quality Expert (LQE)
Grünenthal GmbH Austria

13-OCT-2017

Date

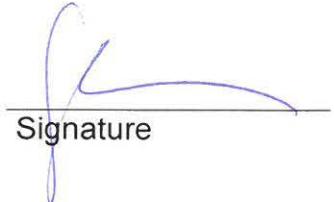
M. Kubista-Andersson

Signature

Reviewed by Susanne Geier
Reg. Affairs and Quality
Manager
(LQE-Deputy)
Grünenthal GmbH Österreich

16-OCT-2017

Date



Signature

Reviewed by Mag. Sibylle Karpf
Medical & Drug Safety
Manager
Local Responsible Person for
Pharmacovigilance
Grünenthal GmbH Austria

30 OCT 2017

Date



Signature

Approved by RN Dr. Thomas Schöffmann
Country Manager Austria
Grünenthal GmbH Österreich

06/11/17

Date



Signature

**Table of contents**

1	Objective	3
2	Scope	3
3	Responsibilities	3
4	Definitions and abbreviations	4
5	Process Description	6
5.1	Collection of Personal Data	6
5.2	Processing of Personal Data	7
5.3	Data Transfer	9
5.4	Data Security	9
5.5	Notification to Authorities	9
5.6	Training	10
6	Cross references	10
6.1	References to standard procedural documents	10
6.2	Legal references (frames)	10
6.3	Other references	10
7	Attachments	10
8	Historical index	10



1 Objective

This SOP defines Data Protection processes according to Grünenthal's Information Security Governance.

2 Scope

This document applies to all Grünenthal employees in Grünenthal GmbH Austria who are involved in the processing of personal data or sensitive personal data.

3 Responsibilities

All Grünenthal employees have to respect Grünenthal's data privacy standard and applicable laws and regulations in their business activities to protect Grünenthal from exposure to potential breaches. This requires employees to take full responsibility for adherence to this SOP.

Grünenthal, as a company, is responsible for ensuring the correct handling of personal data by Grünenthal and any third party engaged to act on Grünenthal's behalf. Grünenthal employees contracting third parties must verify and secure the correct handling of personal data by those third parties.

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

Role	Responsibility
Data Protection Coordinator	<p>Data Protection contact within the local Grünenthal department or affiliate, who within their organisation or function:</p> <ul style="list-style-type: none">- Provides guidance to employees on how to follow the Grünenthal Data Protection standards.- Answers employees' 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 local changes in Data Protection regulations applicable.- Supports the implementation of controls and Data Security measures.



Role	Responsibility
Global/local Compliance	Support global/local implementation of this SOP.
Legal department	Perform legal review of Data Protection related topics and provide legal advice.
Senior management	Support and ensure Data Protection standards implementation, training and adequate monitoring in their department or affiliate.

4 Definitions and abbreviations

Definitions and abbreviations of terms used in this document are explained here.

Term	Definition/Explanation
Consent	Permission received from a data subject on the processing of his/her personal data/sensitive personal data.
Data Controller	A natural or legal person, public authority, agency or any other body which determines the purposes for which and the manner in which any personal data are, or are to be processed.
Data Processing	Any operation or set of operations which is performed upon personal data and sensitive 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 or disposal.
Data Protection	The act of ensuring that the collection and use of Personal Data is limited to the minimum necessary, that individuals should also be clearly informed in a transparent way on how, why, by whom, and for how long their data is collected and used and that people should be able to give their informed consent to the processing of their personal data. <i>Data Privacy is a synonym for Data Protection, used in European guidelines and laws.</i>



Term	Definition/Explanation
Data Transfer	The disclosure, transmission or process of making personal data available between Grünenthal entities and between Grünenthal and third parties or to the public.
Data Subject	Each identified or identifiable, directly or indirectly, natural or legal 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.
Personal Data	Information about an identified or identifiable natural or legal person regardless of the format in which it is displayed (hardcopy or digital). With this kind of data a living individual or legal entity 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.
Sensitive Personal Data	Information or an opinion about an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; or criminal record. Sensitive personal data also includes health information and genetic information about an individual.



5 Process Description

This SOP defines processes and responsibilities for Grünenthal's Data Protection standards as specified in the following sections.

There are 4 major data subject groups on which we handle personal data at Grünenthal:

- Employee data (e.g.: data on 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 (and third party collaborating with Grünenthal, e.g.: healthcare professionals, partners, consultants).
- Data from any other individual or legal entity outside the three groups mentioned above (e.g.: job applicants data).

When handling personal data, we need to comply with the next legal requirements and company standards:

5.1 Collection of Personal Data

To collect, process, use and transfer personal data, it must be:

- expressly permitted and provided by law (e.g. employee's contract) or
- the data subject must have given, in advance, his informed consent.

Personal Data must be collected directly from the data subject, unless the data subject has made such data available through generally accessible sources.

Consent must be:

- Unambiguous
- Voluntarily expressed
- Detailed, as a minimum should contain:
 - o Name and address of the data controller (Grünenthal legal entity)
 - o Purpose of collection, processing or use
 - o Personal data to be collected (e.g.: name, date of birth, DNA etc.)



- Names of recipients who will receive or access the data
- A reference to the data subject's right to withdraw his/her consent.

This consent can be collected as follows:

- Written consent
- eConsent (created for online solutions on website, ipad, etc.)
- Verbal consent (in exceptional cases e.g. adverse event reporting via phone)
- Implicit consent (Consent that is inferred from signs, actions, or facts, or by inaction or silence. E.g.: use of cookies, giving a business card, etc). However, implicit consent is not valid for the processing of sensitive personal data; in this case the data subject has to consent explicitly.

The consent can be withdrawn by the data subject at any time.

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

Sensitive personal data must not be collected, unless:

- the data subject gives explicit consent.
- the personal data concerned relates to data which is manifestly made public by the data subject.
- there is an existing legal requirement to collect the data concerned.

When sensitive personal data needs to be collected, processed, used or transferred, the responsible Grünenthal employee must liaise with the local Data Protection Coordinator to conduct an evaluation of the necessity of data and the right level of protection.

5.2 Processing of Personal Data

Employees must follow the following rules when processing (sensitive) personal data:

5.2.1 Rule of Specific Purpose

Personal data must be processed and used only for the purposes for which they were collected.



Employees must define understandable company purposes for the collection, processing and usage of personal data prior to those actions. 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 and sensitive personal data must be kept only as long as is necessary to satisfy the purposes for which it was intended. They must be disposed 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.

Personal data and sensitive personal data that were collected for different purposes must not be combined or cross-referenced.

5.2.2 Rule of Necessity

Employees must collect only the minimum personal data needed to achieve the defined purpose.

5.2.3 Rule of Transparency

Data subjects can contact anyone within Grünenthal to:

- Be informed about his/her personal data held by Grünenthal;
- Withdraw his/her consent to process his/her personal data at any moment: Grünenthal must delete his/her information from all Grünenthal systems upon request and send a confirmation to the data subject.
- Modify and rectify incorrect data: Grünenthal must modify the incorrect personal data and send a confirmation to the data subject with the changes performed. Sensitive personal data must be deleted, if Grünenthal is unable to prove their accuracy.

Any external request from a data subject to obtain his personal data held by Grünenthal must be submitted immediately to the Data Protection Coordinator and/or Global/local Compliance for follow-up, so Grünenthal can provide the data subject the data Grünenthal holds on him, respecting the timelines set by local regulation, i.e. in Austria within 8 weeks starting from the day on which Grünenthal receives the request.

Any request from an employee on his personal data held by Grünenthal must be submitted to and provided by the employee's HR contact person, respecting the timelines stated by local regulation (in Austria 8 weeks).



5.3 Data Transfer

If personal data are transferred between Grünenthal entities and between Grünenthal and third parties or published, employees must ensure that:

- the Data Protection Coordinator and Global/local Compliance Department has been contacted in order 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:
 - o required for any legal purpose (e.g.: court case)
 - o covered by informed consent
- standard data protection annex, developed by HQ or local, is included in any agreement with External 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, and limited to the specific purpose which Grünenthal received consent for.

5.4 Data Security

Departments involved in the processing of data in any way, must implement the technical and organisational measures required to guarantee compliance with the provision of the Data Protection regulation.

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 application used by Grünenthal needs to be reviewed by the GRT IT department with respect to the GRT "IT Demand management Guideline" to fulfill data protection and other data security obligations.

5.5 Notification to Authorities

In Austria, data processing procedures ("data applications") need to be registered with the Data Protection Authority. This obligation does not apply to standard data applications. Inasmuch as sensitive data are processed the Data Protection Authority needs to approve the processing.



5.6 Training

All employees must complete the training on Information-Security which also contains the principles of Dataprotection via elearning including an online comprehension test. Whenever changes occur in processes or legislative concerning dataprotection a refresher training must also be provided to ensure compliance with the Grünenthal data protection standards.

6 Cross references

Not applicable

6.1 References to standard procedural documents

GRT Code of Conduct in the current version

GL-CM-070-0003-01 Information Security Policy

GL-IT-000-0007-01 Acceptable Use of IT systems

GRT IT Demand Management Guideline

6.2 Legal references (frames)

Local Laws and regulation: Data Protection Act 2000 ("DSG 2000"), Regulation on Standard and Template Applications 2004 ("StMV 2004")

European Directive

6.3 Other references

Not applicable

7 Attachments

Not applicable

8 Historical index

Version/ document no.	Description of changes	Valid from
01	Initial version	see 1 st page