

# Data Processing Agreement (DPA) for the carried out by EXTEDO for the subscription to SafetyEasy™ Database.

between

**Customer**

- hereinafter called “**Controller**” -

and

EXTEDO GmbH, Einsteinstraße 30, 85521 Ottobrunn, Germany

- hereinafter called “**Processor**” -

## §1 Subject matter and duration of the DPA.

### 1. Subject matter and roles

The Subject matter of this DPA is the execution of the services or tasks by EXTEDO GmbH as a processor whenever those activities involve the processing by EXTEDO of the Customer Data in the frame of the subscription to the Software Package.

For the purposes of this DPA, Customer Data must be considered as defined in the General Terms for the subscription to the Software Package and understood as data that has been initially collected and processed by the Controller, for the purposes and means defined by the Controller.

For purposes of this DPA, You and Extedo agree that You are the controller and Extedo is the processor of such Personal Data, and exceptionally when You act as a processor of Personal Data, Extedo will act as a sub-processor.

### 2. Duration

The duration of this DPA corresponds to the duration of the subscription of the Controller to the Software Package “SafetyEasy”.

## §2 Specification of the DPA

### 1. Nature and Purpose of the intended Processing of Data

Within the range of services included in the Software Package and additional related services, the processing activities that EXTEDO performs and may handle personal data shall comprise:

- Set up assistance

- Data migration services might be required for the implementation of the Databases. The coordination of the migration project is shared between EXTEDO and the Service Provider Ab Cube.
- First and Second Level support: the main activity that EXTEDO will perform upon personal data implies remote intervention of an EXTEDO's employee to the controller upon request of the Controller. In some cases, these services might also be delivered by the Service Provider AB CUBE. If so, the corresponding information and additional DPA will be available to the Controller and shall govern the activity jointly with this DPA.
- One-time services: training and validation if required.
- Additional services: consulting services that can be ordered with a separate request of the Customer and might also involve access to Customer Data by EXTEDO's personnel.

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Controller and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled. The adequate level of protection in the United States is the result of Standard Data Protection Clauses (Article 46 Paragraph 2 Points c and d GDPR) in place with EXTEDO's Affiliate in the United States.

## 2. Type of Data

The Subject Matter of the processing of personal data might comprise the following data categories:

- data related to the identity and contact details of the patients
- data related to the identity and contact details of the health professionals
- data related to the health of patients
- data related to adverse effects of the patients

## 3. Categories of Data Subjects

The Categories of Data Subjects comprise those individuals whose data are collected and/or provided by the Controller or its provider to EXTEDO or its Service Provider, for example the data concerning patients testing the effects of the drugs and healthcare professionals.

### **§3 Technical and Organisational Measures**

1. Before the commencement of processing, EXTEDO shall document the execution of the necessary Technical and Organisational Measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Controller for inspection. Upon acceptance by the Controller, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Controller shows the need for amendments, such amendments shall be implemented by mutual agreement.

2. EXTEDO shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. [Details in Attachment 1]
3. The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for EXTEDO to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

#### **§4 Rectification, restriction and erasure of data**

1. EXTEDO may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Controller, but only on documented instructions from the Controller. In the event of a Data Subject contacts EXTEDO directly concerning a rectification, erasure, or restriction of processing, EXTEDO will immediately forward the Data Subject's request to the Controller.
2. Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by EXTEDO in accordance with documented instructions from the Controller without undue delay.

#### **§5 Quality assurance and other duties of EXTEDO**

In addition to complying with the rules set out in this DPA, EXTEDO shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, EXTEDO ensures, in particular, compliance with the following requirements:

- a) Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR. The DPO can be reached at the following email address ([privacy@extedo.com](mailto:privacy@extedo.com)).
- b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. EXTEDO entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. EXTEDO and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Controller, which includes the powers granted in this contract, unless required to do so by law.

- c) Implementation of and compliance with all Technical and Organisational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in Attachment 1].
- d) The Controller and EXTEDO shall cooperate, on request, with the supervisory authority in performance of its tasks.
- e) The Controller shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as EXTEDO is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.
- f) Insofar as the Controller is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by EXTEDO, EXTEDO shall make every effort to support the Controller.
- g) EXTEDO shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.
- h) Verifiability of the Technical and Organisational Measures conducted by the Controller as part of the Controller's supervisory powers referred to in item 7 of this contract.

## **§6 Subcontracting**

1. Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. EXTEDO shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Controller's data, even in the case of outsourced ancillary services.
2. EXTEDO may commission subcontractors (additional contract processors) only after explicit written or documented consent from the Controller.
  - a) The Controller agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Company	Activity	Service	Purpose
Citrix	Platform provider for remote access via the application "GoToMeeting".	Customer Support	The establishment of a remote connection to the customer for analysing support cases and performance of support tasks.
Microsoft	Office 365	Customer Support	Document management and collaboration

b) Outsourcing to subcontractors or Changing the existing subcontractor are permissible when:

- EXTEDO submits such an outsourcing to a subcontractor to the Controller in writing or in text form with appropriate advance notice. Depending on the geographical area of the Controller, an additional Extedo subcontractor might have access the Customer Data for the purposes listed under §2.1. and exclusively for the service(s) listed below. At the moment, the Controller accepts the following subcontractors list:

Company	Geographical Region	Service (s)
Asphalion	Spain & Germany	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
Bio and Gene	Australia & South Korea,	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
eBIT	Kuwait, Bahrain & Oman	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
eGID	Egypt	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
InfoCert	Italy	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
GGA	Taiwan	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
Inpharmatis LLC	CIS	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
Jiaxing Taimei Medical	China	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
NEOTRIDENT	China	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
Organex Brazil	Brazil, Peru, Mexico & Chile	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer

SIPS	MENA	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
Team Tranquil	US & India	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
Uni.systems	Greece	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer
VtR	Taiwan	1 <sup>st</sup> and 2 <sup>nd</sup> Level Support and Training in the Language of the customer

- The Controller has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to EXTEDO; and
  - The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.
3. The transfer of personal data from the Controller to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.
  4. If the subcontractor provides the agreed service outside the EU/EEA, EXTEDO shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.
  5. Further outsourcing by the subcontractor requires the express consent of the main Controller (at the minimum in text form); All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

## **§7 Supervisory powers of the Controller**

1. The Controller has the right, after consultation with EXTEDO, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by EXTEDO in his business operations by means of random checks, which are ordinarily to be announced in good time.
2. EXTEDO shall ensure that the Controller is able to verify compliance with the obligations of EXTEDO in accordance with Article 28 GDPR. EXTEDO undertakes to give the Controller the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.
3. Evidence of such measures, which concern not only the DPA, may be provided by either auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor), or a suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

4. EXTEDO may claim remuneration for enabling Controller inspections.

### **§8 Communication in the case of infringements by EXTEDO**

1. EXTEDO shall assist the Controller in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:
  - a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
  - b) The obligation to report a personal data breach immediately to the Controller
  - c) The duty to assist the Controller with regard to the Controller's obligation to provide information to the Data Subject concerned and to immediately provide the Controller with all relevant information in this regard.
  - d) Supporting the Controller with its data protection impact assessment
  - e) Supporting the Controller with regard to prior consultation of the supervisory authority
2. EXTEDO may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of EXTEDO.

### **§9 Authority of the Controller to issue instructions**

1. The Controller shall immediately confirm oral instructions (at the minimum in text form).
2. EXTEDO shall inform the Controller immediately if he considers that an instruction violates Data Protection Regulations. EXTEDO shall then be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

### **§10 Deletion and return of personal data**

1. Copies or duplicates of the data shall never be created without the knowledge of the Controller, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.
2. After conclusion of the contracted work, or earlier upon request by the Controller, at the latest upon termination of the Service Agreement, EXTEDO shall hand over to the Controller or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste,

redundant and discarded material. The log of the destruction or deletion shall be provided on request.

3. Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by EXTEDO in accordance with the respective retention periods. It may hand such documentation over to the Controller at the end of the contract duration to relieve EXTEDO of this contractual obligation.

Attachment 1 Technical and Organisational Measures

Ottobrunn, [...]

Processor

Processor

Name: Martin Schmid

Name: ppa. Elmar Weber

Title: Managing Director

Title: VP Finance & Corporate Services

Signature:

Signature:

Controller

Controller

Name:

Name:

Title:

Title:

Signature:

Signature:



## Attachment 1 - Technical and Organisational Measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)
  - Physical Access Control  
No unauthorised access to Data Processing Facilities, e.g.: keys, electronic door openers, alarm systems.
  - Electronic Access Control  
No unauthorised use of the Data Processing and Data Storage Systems, e.g.: secure passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
  - Internal Access Control (permissions for user rights of access to and amendment of data)  
No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events
  - Isolation Control  
Isolated Processing of Data, which is collected for differing purposes through isolated productive, development and test systems; productive Data shall not be used as copy for test purposes; multiple Controller support, sandboxing
  
2. Integrity (Article 32 Paragraph 1 Point b GDPR)
  - Data Transfer Control  
No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN);
  - Data Entry Control  
Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management
  
3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)
  - Availability Control  
Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning
  - Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);
  
4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)
  - Data Protection Management;
  - Incident Response Management;
  - Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
  - Order or Contract Control  
No third party data processing as per Article 28 GDPR without corresponding instructions from the Controller, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.