General Terms and Conditions of Use

General Terms and Conditions of Use of the apotec® Refrigerator Monitoring Service

The object of the present General Terms and Conditions of Use is the apotec® Refrigerator Monitoring Service (hereinafter referred to as "apotec® refrigerator monitoring"), which is supplied by WEPA APOTHEKENBEDARF GmbH & Co. KG (hereinafter referred to as "WEPA").

1. Scope of application

1.1 The following General Terms and Conditions of Use apply exclusively to apotec® refrigerator monitoring. The provider of refrigerator monitoring is WEPA APOTHEKENBEDARF GmbH & Co. KG, Am Fichtenstrauch 6-10, 56204 Hillscheid, represented by its Managing Director Dr. Christian Ciesielski.

1.2 apotec® refrigerator monitoring is solely aimed at users who are acting within the scope of exercising their commercial or self-employed business activity. Other users, in particular consumers within the meaning of § 13 BGB, are excluded from the use of apotec® refrigerator monitoring.

2. Object of apotec® refrigerator monitoring

2.1 apotec® refrigerator monitoring is a digital cloud-based service which enables the switch status of components, alarm statuses and temperatures of one or more professional cooling and freezing appliances to be recorded and visually presented in a browser-based application. Refrigerator monitoring further permits measurement values to be recorded and displayed via external sensors, which can be acquired in various versions as an accessory to the apotec® Refrigerator Monitoring Service.

3. Right of use

3.1 Pursuant to the present General Terms and Conditions of Use, the user is entitled to use apotec® refrigerator monitoring vis-à-vis WEPA only. The right of use is an appliance-related, simple, non-exclusive, non-transferable right of use which is time-limited in accordance with Clause 5.1 below (hereinafter referred to as "apotec® refrigerator monitoring licence").

4. Prerequisites for use and duties of the user

4.1 In order to be able to use apotec® refrigerator monitoring, the user will need to acquire the following at his own expense.

· A cooling and/or freezing appliance which is compatible with apotec® refrigerator monitoring

· An RS 485 plug and an RS 485 adaptor to connect the cooling and/or freezing appliance to the network

· A valid apotec® refrigerator monitoring licence for the respec-tive cooling and/or freezing appliance

· An active WEPA account

4.2 The user commits only to register cooling and/or freezing appliances which are authorised for apotec® refrigerator monitoring by WEPA and further commits to keep his contact details in the apotec® refrigerator monitoring user profile up to date at all times.

4.3 apotec® refrigerator monitoring may only be used with cooling and/or freezing appliances which are authorised for apotec® refrigerator monitoring by WEPA and which are installed and operated within the European Union, the EFTA states or the United Kingdom.

4.4 Cooling and/or freezing appliances which are authorised for apotec® refrigerator monitoring by WEPA may only be connected via the networking solutions authorised by WEPA.

4.5 The user may not use apotec® refrigerator monitoring in an improper manner. In particular, the user is not permitted to circumvent any technical restrictions of apotec® refrigerator monitoring or to pursue unlawful purposes.

5. Term of the contract

5.1 The contract commences upon activation of the licence key in the apotec® refrigerator monitoring and runs for a term of 12 or 36 months depending on the subscription selected. The contractual term applicable to the user on an individual case basis is stated in the order confirmation. The contractual term is automatically extended by the period stipulated above if notice of termination of four weeks to the respective end of the contract is not given.

5.2 The above is without prejudice to the right to terminate the contract for cause. Particular circumstances in which WEPA would have the right to terminate the contract for cause without any requirement to give notice are as follows.

5.2.1 The user breaches the rights of use granted by WEPA by using apotec® refrigerator monitoring beyond the degree permitted in accordance with the present General Terms and Conditions of Use or pursuant to the Licence Terms and does not cease and desist within an appropriate deadline following a warning from WEPA.

5.2.2 The user is in arrears of two months or more in respect of payment of the remuneration due.

5.2.3 The user suffers a material deterioration or faces an impending material deterioration in his financial situation. This particularly applies where the user has applied for insolvency proceedings to be instigated in respect of his assets or where insolvency proceedings have been initiated in respect of his assets.

5.2.4 The cooperation partner Liebherr-Hausgeräte Vertriebs- und Service GmbH no longer provides WEPA with the performances agreed vis-à-vis WEPA (e.g. following termination of contractual arrangements) and WEPA is, as a consequence, no longer able to offer the service due.

5.3 Notices of termination are not valid unless given in writing. Compliance with the written form is a prerequisite for the effectiveness of the notice of termination.

5.4 Upon the termination of the contract, WEPA will deactivate the service in the WEPA cloud and cancel the access authorisation of the user to this service.

6. User fee

6.1 The remuneration to be paid by the user is stipulated in the order confirmation. All prices are stated in EUR and are subject to Value Added Tax at the statutory rate.

6.2 Payment terms are stipulated in the order confirmation.

6.3 WEPA may act at its own just and fair discretion (§ 315 Paragraph 3 German Civil Code BGB) in adjusting the user fee pursuant to Clause 6.1 above in line with the development of costs determining the price calculation. The licence fees which WEPA is required to pay for the operation of apotec® refrigerator monitoring are particularly material to the price calculation. WEPA will notify the user of any increases in remuneration in a timely manner and in writing and will do so no later than 3 months before such an increase enters into force. A price increase may not exceed the previous remuneration by more than 10%.

In the event of a price increase, the user is entitled to give written notice of termination of the contract within 3 months of receipt of such an announcement in accordance with sentence 2 above. WEPA will expressly indicate this opportunity to give notice of termination in its announcement pursuant to sentence 2 above. The new user fee announced by WEPA will apply if no notice of termination is given within this deadline.

7. System changes

7.1 WEPA is entitled to make changes to apotec® refrigerator monitoring within the scope of product development and is in particular entitled to adapt apotec® refrigerator monitoring to legal, statutory, economic and technical conditions.

8. Liability

8.1 User compensation claims for damages of any kind are excluded. Said limitation of liability further applies in favour of statutory representatives and vicarious agents of WEPA insofar as the user asserts claims against these parties.

8.2 Claims for compensation which result from intentional or grossly negligent breach of duty on the part of WEPA or on the part of a statutory representative or vicarious agent of WEPA are excluded from the above limitation of liability. Breach of material contractual duties which at least amounts to ordinary negligence is also excluded from the above limitation of liability. Material contractual duties are such duties as are required to be fulfilled for the proper execution of the contract in the first place and constitute duties which the user may ordinarily rely upon to be fulfilled.

8.3 The above limitation of liability is without prejudice to liability pur-suant to a peremptory norm, in particular liability pursuant to the Product Liability Act, and is further without prejudice to liability in the event of culpable harm to life, limb or health of the user.

9. Availability

9.1 There is no right to uninterrupted use. No guarantee is given that access to or use of apotec® refrigerator monitoring will not be interrupted or adversely affected by maintenance works, further developments or otherwise because of malfunctions. WEPA will endeavour to make apotec® refrigerator monitoring available for use in a way which is as free from interruption as possible and will notify the user in advance of planned maintenance works. Notwithstanding this, temporary restrictions or interruptions may occur as a result of technical malfunctions (such as interruption of the power supply, hardware and software errors, technical problems in the data lines).

10. Data privacy

10.1 The parties commit to processing personal data in accordance with the relevant provisions under data protection law.

10.2 Insofar as WEPA processes personal data of employees of the user in connection with provision of performance, the parties agree that the handling of such personal data will be governed by a processing agreement pursuant to Article 28 GDPR which is attached as Annex 1.

11. Copyright, labelling rights and other intellectual property

11.1 The contents retrievable in apotec® refrigerator monitoring (texts, data, pictures, logos, graphics, documentations, sound, video and other pictorial depictions) are subject to copyright and to other laws governing the protection of intellectual property. Said contents may not be reproduced, disseminated, stored in other media (e.g. other websites) or changed, either in whole or in part, without the express prior consent of the respective rights holder.

12. Amendments to the General Terms and Conditions of Use

12.1 WEPA reserves the right to amend individual clauses contained within the present General Terms and Conditions of Use with future effect and without any requirement to state grounds for so doing insofar as such amendments take account of the interests of WEPA and are reasonable for the user. WEPA will notify the user in a timely fashion of any amendments to the General Terms and Conditions of Use. The amended General Terms and Conditions of Use will be deemed to have been accepted if the user does not object to an amendment to the General Terms and Conditions of Use within six weeks of the entry into force of such an amendment. In the event that the user objects to amendments, WEPA will be entitled to act in the interests of the user by terminating the use agreement in circumstances where adherence to contractual relations is not possible or not reasonable if the previous General Terms and Conditions of Use continue to apply.

13. Final provisions

13.1 The present General Terms and Conditions of Use and interpretation of the present General Terms and Conditions of Use are solely governed by the law of the Federal Republic of Germany. Application of German and European civil law and application of the UN Convention on Contracts for the International Sale of Goods (CISG) are excluded.

13.2 The location of the Registered Office of WEPA is the sole place of jurisdiction for all disputes arising from or in conjunction with the present General Terms and Conditions of Use.

13.3 In the event that individual provisions contained within the present General Terms and Conditions of Use are invalid and/or unenforceable, this shall be without prejudice to the validity of the other provisions herein contained. Supplementary interpretation of the contract will involve the replacement of invalid and/or unenforceable provisions by such valid and enforceable provisions as are most suitable to achieve the economic purpose pursued and accord due consideration to the vested interests of both parties. The same will apply in respect of gaps in provision within the present General Terms and Conditions of Use.

Status: 04/2024

Annex 1: Agreement on Data Processing pursuant to Article 28 GDPR

Insofar as WEPA (hereinafter in this Annex referred to as the "processor") processes personal data of employees of the user (hereinafter referred to as the "controller"), this shall be governed by the stipulations regarding processing set out below.

1. Purpose and scope of application

1.1 The present Agreement on Data Processing (hereinafter referred to as "standard contractual clauses") is essentially based on the standard contractual clauses listed in the Annex to the COMMISSION IMPLEMENTING DECISION (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council.

1.2 The aim of these standard contractual clauses is to ensure compliance with Article 28 Paragraphs 3 and 4 of 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 Directive 95/46/EC (General Data Protection Regulation).

1.3 The parties have agreed to these standard contractual clauses in order to ensure compliance with Article 28 Paragraphs 3 and 4 of Regulation (EU) 2016/679.

1.4 The standard contractual clauses apply to the processing of personal data in accordance with Annex I.

1.5 Annexes I to III are a component part of the standard contractual clauses.

1.6 These standard contractual clauses apply notwithstanding the obligations to which the controller is subject pursuant to Regulation (EU) 2016/679.

1.7 In and of themselves, these standard contractual clauses do not ensure that duties in connection with international transfers of data pursuant to Chapter V of Regulation (EU) 2016/679 are fulfilled.

2. Interpretation

2.1 If the terms defined in Regulation (EU) 2016/679 are used in the pre-sent standard contractual clauses, they will have the same meaning as in the relevant Regulation.

2.2 These standard contractual clauses are to be interpreted in light of the provisions contained in Regulation (EU) 2016/679.

2.3 These standard contractual clauses may not be interpreted in a way which runs contrary to the rights and duties stipulated in Regulation (EU) 2016/679 or in a way which infringes the basic rights or basic freedoms of data subjects.

3. Description of processing

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex I.

4. Obligations of the parties

4.1 Instructions

4.1.1 The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of such a legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

4.1.2 The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

4.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex I, unless it receives further instructions from the controller.

4.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex I.

4.4 Security of processing

4.4.1 The processor shall at least implement the technical and organisational measures specified in Annex II in order to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or unauthorised access to the data (hereinafter referred to as a "personal data breach"). In assessing the appropriate level of security, the parties shall take due account of the state of the art of the technology, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

4.4.2 The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.6 Documentation and compliance with the standard contractual clauses

4.6.1 The parties shall be able to demonstrate compliance with the present standard contractual clauses.

4.6.2 The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with the present standard contractual clauses.

4.6.3 The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in the present standard contractual clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by the present standard contractual clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifi-cations held by the processor and/or by a subprocessor.

4.6.4 The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor. For the purpose of conducting inspections, the controller is entitled to enter business premises of the processor at which personal data is being processed on behalf of the controller during usual business hours and after having given reasonable notice (generally at least 14 calendar days) to the extent that an inspection without notice does not appear strictly necessary for the auditing purpose. The inspection is carried out at the controller's expense and may not disproportionately impede business operations. Strict confidentiality must be maintained in respect of the operating and business secrets of the processor. Inspections are limited to once per calendar year in all cases. This is without prejudice to inspections for a compelling reason which the controller is required to demonstrate. The processor will bear the cost of the audit to the extent that an audit has been rendered necessary by an infringement of the law or contractual breach by the processor.

4.6.5 If the controller mandates an independent auditor to conduct the audit, the controller will obtain from such an independent auditor a writ-ten undertaking which imposes the same obligations as are incumbent on the controller vis-à-vis the processor pursuant to the present Clause 4.6. In addition to this, the controller is required to impose a duty of confidentiality and secrecy on the independent auditor unless the independent auditor is already bound by a professional duty of confidentiality. At the request of the processor, the controller is required to submit the confidentiality agreements entered into with the independent auditor to the processor without delay. The controller may not engage a competitor of the processor to conduct an inspection.

4.6.6 Having accorded due consideration to the statutory duties of the controller, the processor is entitled to act at its own fair and just discretion in not disclosing information which is sensitive with regard to the business of the processor or in withholding information which, if disclosed, would be in breach of statutory or other contractual provisions. The controller is not entitled to receive access to data or information on other customers of the processor, to information regarding costs, quality audits and contract management reports or to any other contractual data of the processor which is not of direct relevance to the audit purposes agreed.

4.7 Use of sub-processors

4.7.1 The processor has the controller's general authorisation for the engagement of sub-processors from the agreed list provided in Annex III. The processor shall specifically inform the controller in writing of any intended changes of said list through the addition or replacement of sub-processors at least 14 calendar days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s) concerned. The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

4.7.2 Where the processor engages a sub-processor for the carrying out of specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with the present standard contractual clauses.

4.8 International data transfers

The controller agrees that where the processor engages a sub-processor in accordance with Clause 4.7 for the carrying out of specific processing activities (on behalf of the controller) and where such processing activities involve a transfer of personal data within the meaning of Chapter 5 of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter 5 of Regulation (EU) 2016/679 by using a security mechanism pursuant to Article 44 ff. of the GDPR (in particular an adequacy decision or standard contractual clauses adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679).

5. Assistance to the controller

5.1 The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

5.2 The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights whilst taking the nature of the processing into account.

5.3 In addition to the processor's obligation to assist the controller pursuant to Clause 5.2, the processor shall furthermore assist the controller in ensuring compliance with the obligations set out in Articles 32 to 36 whilst taking the nature of the data processing and the information available to the processor into account.

6. Notification of personal data breaches

In the event of a personal data breach, the processor shall cooperate with and assist the controller in complying with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 whilst taking the nature of the data processing and the information available to the processor into account.

7. Non-compliance with the standard contractual clauses and termination of the contract

7.1 In the event that the processor is in breach of its obligations under present standard contractual clauses and without prejudice to the provisions contained within Regulation (EU) 2016/679, the controller may instruct the processor to suspend the processing of personal data until such time as the latter is in compliance with the present standard contractual clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with the present standard contractual clauses for whatever reason.

7.2 The controller shall be entitled to terminate the contract insofar instructions issued by the controller are in breach of Regulation (EU) 2016/679 or in breach of the applicable Union or Member State data protection provisions and insofar as the controller insists on compliance with such instructions having been notified by the processor that its instructions are in breach of applicable legal requirements pursuant to Clause 4.1.2 above.

7.4 Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with the present standard contractual clauses.

ANNEX I - Description of processing

Categories of data subjects whose personal data is processed

- Employees of the controller

Categories of personal data which is processed

- Log files, any IP addresses, user principal name (UPN), date and time of access and type of access, type and version of browser used, operating system used, URL of the portal site at the time of access, actions undertaken on the portal, access of backend services
- Authentication data, such as user principal name (UPN), company address, company ID, first name and surname, e-mail address, telephone number
- Appliance data of the cooling and freezing appliances and of the smart module, such as model, serial number, article number and telemetric data including temperature, door opening status, network data (e.g. Mac and IP address smart modules, (W)LAN status)
- Notification functions e-mail (user principal name, UPN, company ID, e-mail address of the recipient, meta data relating to the messages, content of the message, company address, links to reports)
- Notification functions SNS and calls (user principal name, UPN), company ID, telephone number of the recipient, meta data relating to the messages, content of the message or of the call notification)

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (in-cluding access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

- No sensitive data is processed.

Nature of data processing

- Nature of data processing is specifically described in the General Terms and Conditions of Use. Continuous recording of temperatures, alarm statuses and switch status of components is ensured via the browser-based application. An alert can be set in the case of a temperature which is too high or too low. The alert can take place via e-mail or SMS notification. Reports can also be drawn up and downloaded in order to be able to fulfil various duties of documentation that may apply.

Purpose(s) for which the personal data is processed on behalf of the controller

- Safeguarding of stability and of network and information security
- Authentication on the portal within the scope of use
- User and permissions management on the portal
- Dispatch of notifications
- Transmission of reports via digital means
- Last language chosen for the portal, internationalisation of the log-in
- Storage of log-in data after a successful log-in (e.g. name, UPN, to-kens)

Duration of processing

- Duration of processing corresponds to the term of the use agreement.

ANNEX II - Technical and organisational measures including technical and organisational measures to ensure the security of the data

For provision and hosting of the portal, the processor uses the services of the sub-processor, whose technical and organisational measures are set out below.

1. Confidentiality

1.1 Entry control

Aim: No unauthorised entry to data processing facilities

- Automatic access control system, badge reader
- Chip cards/transponder systems
- 2-factor locking system at the data centre (biometrics)
- Entry regulations for admission to the data centre
- Manual locking system
- Security locks
- Key regulations/list/documentation
- Door protection
- Doors with knobs on the outside
- Electronic doors
- Main entrances closed outside office hours
- Entry only possible with badge
- Visitor access via reception only
- Visitor log
- Works fully fenced in
- Barriers/turnstiles
- Staff and visitor badges
- Visitors accompanied by employees
- Personal collection of visitors
- Security guards in place to secure the site
- Security cameras
- Careful selection of security staff

1.2 Access control

Aim: No unauthorised system use

- Log-in with user name + password
- Password Policy
- General IT security policy (Computer Use Policy, Password Policy, Account Policy, Mobile Device Policy etc)
- Automatic desktop screen lock
- Next Generation Anti-Virus-Software Clients
- Next Generation Anti-Virus-Software Server
- BIOS protection (with PIN/password)
- Locking of external interfaces
- Encryption of notebooks/tablet
- Encryption of data carriers
- Management of user permissions
- Identity Access Management System
- Encryption of smart phones

- Mobile Device Management
- Network access control LAN/WIFI (NAC)
- Firewall
- Use of VPN technology
- Creation of user roles
- Password management system

1.3 System access control

Aim: No unauthorised reading, copying, changes or removals within the system

- Use of permissions concepts
- Management of permissions by administrators
- Approval of permissions by data owners
- Minimum number of system administrators/application administrators
- Secured use of USB interfaces
- Secure storage of data carriers
- Safe for back-ups
- Proper destruction of data carriers
- External document shredding or service providers acting in accordance with the current stipulations of Data Policy
- Document shredders
- Logging of access to applications/servers

1.4 Separation control

Aim: Separate processing of data which has been collected for different purposes

- Separation of production and test environment
- Physical separation (systems/databases/data carriers)
- Control via permissions concept
- Regular scrutiny of permissions
- Separation of data and systems/applications
- Multi-client capability of relevant applications
- Stipulation of database rights

1.5 Pseudonymisation

Aim: Processing of personal data in a way which ensures that data can longer be attributed to a data subject without the employment of additional information as long as this additional information is stored separately and is subject to relevant technical and organisational measures

- Transmission of data in anonymised, pseudonymised or encrypted form
- Internal instruction regarding the careful handling of personal data
- Deletion of personal data after expiry of the statutory deletion deadline
- Separation of assignment data

2. Integrity

2.1 Transfer control

Aim: No unauthorised reading, copying, changes or removals in the case of electronic transmission

- E-mail encryption during transport (within the group)

- Use of dedicated connections
- Use of VPN
- Data carrier asset and assignment to persons
- Logging of access and retrievals
- Secure transport containers
- Provision via encrypted connection
- Careful selection of transport staff and vehicles
- Personal handover with log and signature
- Use of signatures
- Use of certificates

2.2 Data entry control

Aim: Ascertain whether and by whom data has been entered into processing systems, changed or removed

- Technical logging of entry, changing and deletion of data
- Regular plausibility checks
- Retention and deletion deadline
- Clear areas of responsibility for deletions
- Traceability of entry, change and deletion of data by individual user names
- Issuing of rights for the entry, amendment and deletion of data on the basis of a permissions concept with data owners and approvals
- Logging of changes which are added to automatic processings

3. Availability and robustness

Aim: Protection against accidental or deliberate destruction or loss

- Server and storage systems in a secure data centre
- Data centre air conditioned
- Fire and smoke alarms and early fire detection
- Data centre monitors temperature and humidity
- Camera surveillance in the data centre
- Reports upon entry to the data centre
- No sanitary facilities in the data centre
- Fire extinguishers in and/or outside the data centre
- Redundant UPS systems
- Protection against environmental impacts (storm, water)
- RAID system/hard disk mirroring
- Separate partitions for operating systems and data
- Regular software updates
- Regular carrying out of a weak point analysis for hardware and software
- Virus protection system
- Back-up and recovery concept
- Control of the back-up process
- Regular tests for data restoration and logging of results
- Existence of an emergency plan
- Storage of back-up media in a secure place outside the data centre
- Data protection safe

4. Procedures for regular monitoring, assessment and evaluation

Data protection management

- Internal data protection officer:
- Data protection organisation/data protection management
- Data protection guide/recommendations
- Central documentation of all processing activities and data protection rules which can be accessed by employees if needed/if they hold the right permissions
- Formalised process for the processing of information enquiries by data subjects is in place
- Data privacy assessments are conducted as and when required
- Employees receive training on/are made aware of data protection
- Employees bound by confidentiality/data secrecy

IT security management

- Internal IT security officer
- Information security management system
- Liebherr IT Security Policies
- Regular IT security audits
- Employees trained in data security

Incident response

- Intrusion Prevention System (IPS)
- Deployment of a firewall and regular updating
- Deployment of a spam filter and regular updating
- Deployment of a virus scanner and regular updating
- Documented approach to dealing with security incidents
- Documentation of security incidents and data failures
- Involvement of the data protection officer and IT security officer in security incidents and data failures
- Formal process and areas of responsibility for the post-processing of security incidents and data failures
- Documented process for the recognition and reporting of security incidents/data breaches (including in respect of reporting duties to supervisory authorities)

Data protection-friendly default approaches

- Personal data is now only collected as necessary for the respective purpose
- Simple exercising of right of withdrawal by data subjects via technical measures

Assignment control

- Existing sample agreements for processing
- Defined process for clear contract structuring
- Careful selection of processors
- Scrutiny of agreements
- Control of contract execution

ANNEX III - List of sub-processors

The controller has approved the use of the following sub-processors:

Name	Address	Contact person	Description of processing
Liebherr-Hausgeräte Vertriebs- und Service GmbH	Konrad-Zuse-Straße 4+6, 89081 Ulm, Germany		Provision and hosting of the portal:
Liebherr-Hausgeräte Ochsenhausen GmbH (as sub-processor of der Liebherr-Hausgeräte Vertriebs- und Service GmbH)	Memminger Straße 77-79, 88416 Ochsenhausen, Germany		Hosting Azure Cloud, provision and technical management of the portal, authentication, licence management

General Terms and Conditions of Use

WEPA Apothekenbedarf
GmbH & Co KG, D-56204 Hillscheid
www.wepa-apothekenbedarf.de

T +49 (0)2624 107-361
F +49 (0)800 5252500 (gebührenfrei)
info@wepa-apothekenbedarf.de

wepa.shop
wepa.cloud
wepa.school