retarus

Data processing agreement ("DPA") pursuant to Article 28 GDPR

Preamble

The service provisioning by Retarus (hereinafter: "Processor") to the Customer (hereinafter: "Controller"), as agreed in the Individual Order, includes, inter alia, the processing of personal data. The regulations of this DPA shall apply to the processing of personal data by Processor in the course of its service provisioning and, in this respect, specify the Parties' obligations in terms of data protection law.

1. Subject matter and term of the order

(1) Subject matter of the order is the provisioning of services as described in the Individual Order.

(2) This order shall have the same term as the Individual Order. Accordingly, this order terminates with the expiration or termination of the Individual Order.

2. Specification of order details

(1) Nature and purpose of the intended processing

Nature and purpose of Processor's tasks consist in the provision of communication related services, as described in greater detail in the Individual Order.

The performance of the contractually agreed processing 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). Any transfer of personal 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 Articles 44 et seq. GDPR have been fulfilled. Controller's agreement shall not be unreasonably withheld or delayed.

(2) Types of personal data

The subject matter of the processing comprises the following data types:

☒ Personal master data

☒ Communication data (e. g. telephone, e-mail, fax)

☐ Key contract data

☐ Contract billing and payments data

☐ _____

(3) Categories of data subjects

The following categories of data subjects are affected by the processing:

☒ Recipients and senders of messages addressed to or sent by Controller

☒ Controller's employees / contact persons

☐ Customers

☐ Suppliers

☐ Board of managers

☐ _____

3. Technical and organisational measures

(1) The Processor shall implement technical and organizational measures according to Article 32 GDPR for an appropriate protection of Controller's data, which shall ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. (The measures to be implemented by Processor are specified in greater details in the annex to this DPA.)

(2) The technical and organizational measures are subject to technological progress and further developments. To that extent, Processor may at any time implement suitable alternative measures, provided that the security level of the measures shall not be lowered. Substantial changes shall be documented.

4. Data subjects' rights

(1) The Processor may not on its own authority rectify, erase or restrict the data that is being processed on behalf of Controller, but only on documented instructions from the Controller. Insofar as a data subject contacts the Processor directly concerning the rectification / erasure of data, the restriction of processing or a request for information, the Processor will immediately forward the data subject's request to the Controller.

(2) The Processor shall, in accordance with Controller's instructions, reasonably assist the Controller in the implementation of Controller's erasure policy as well as in the handling of data subjects' requests with regard to their rights (e.g., in terms of rectification, data portability, erasure and access).

5. Quality assurance and further obligations of Processor

The Processor shall meet the requirements as specified below:

a) Designation of a data protection officer performing its tasks according to Articles 38 et seq. GDPR.

The Processor has designated a data protection officer who can be contacted by e-mail:

dataprivacy@retarus.com

Further contact information is easily accessible on the Processor's website.

b) Periodical monitoring of the internal processes and the technical and organizational measures pursuant to Section 3 above, in order to ensure that processing within Processor's area of responsibility is in accordance with the requirements of applicable data protection law, taking account, in particular, without limitation, of the protection of the data subjects' rights.

c) The Processor ensures that (i) its employees entrusted with the processing of Controller's data and (ii) other persons acting on Processor's behalf must not process the data unless on instructions from the Controller. Further, the Processor ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

d) The Processor will inform the Controller immediately in case Controller's data is jeopardized by seizure, insolvency proceedings or other events or by measures of a third party. The Processor shall, without undue delay, inform all persons responsible in this context that the data solely belongs to Controller as the "controller" within the meaning of the GDPR.

6. Subcontracting

(1) Subcontracting for the purpose of this Section 6 is to be understood as the commissioning of 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 as well as measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Processor 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) The Processor may commission subcontractors (additional processors) only after prior consent from the Controller. Controller's consent may only be withheld for a compelling reason regarding data protection law.

(3) Controller's consent to the commission of a subcontractor shall be deemed given, if (i) the Processor has informed the Controller in writing or in text form about the planned commission of a certain subcontractor and (ii) the Controller has not objected against the respective commission in writing or in text form within 14 calendar days upon receipt of the information.

(4) In case the Controller withholds consent to the commission of a subcontractor without a compelling reason regarding data protection law, the Processor may terminate the Individual Order, taking into account a reasonable phase-out time. Insofar as the Individual Order comprises different services, which are separable from each other and may be used by Controller independently from each other, the termination right shall only apply to those parts of the Individual Order, which are affected by the Controller's refusal to consent to the respective commission.

(5) The reasonable phase-out time within the meaning of paragraph (4) above is six (6) months as a maximum or the remaining term of the Individual Order, whichever is shorter.

(6) The Controller hereby agrees to the commissioning of the following subcontractor:

- retarus GmbH, Aschauer Straße 30, 81549 Munich, Germany

(7) If and to the extent that services in the field of EDI and/or OCR are subject matter of the Individual Order, the Controller hereby agrees to the commissioning of the following subcontractors:

- Ametras Documents GmbH, Salbeiweg 1, 88436 Eberhardzell, Germany
- retarus (Romania) S.R.L., Piața Consiliul Europei, Nr. 2A, United Business Center 1, Sp. U1P3, 300627 Timisoara, Romania

(8) If and to the extent that services in the field of E-Mail Security are subject matter of the Individual Order, the Controller hereby agrees to the commissioning of the following subcontractor:

- Bitdefender S.R.L., Orhideea Towers Building, 15A Orhideelor Avenue, 6th District, 060071 Bucharest, Romania

(9) In the event of Processor commissioning a subcontractor, the Processor shall impose his data protection obligations as set out in this DPA on the subcontractor by way of a contract according to Article 28 (2) – (4) GDPR.

7. Supervisory powers of Controller

(1) The Processor shall provide evidence of his compliance with the Processor's obligations as set out in Article 28 GDPR by appropriate means, in particular, without limitation, by providing the necessary information in each case.

(2) If an inspection on Processor's business premises should be necessary in an individual case, the inspection will be carried out – whether by Controller or an inspector engaged by Controller – after at least ten calendar days' prior notice, during Processor's normal business hours without disturbance of the operating procedures. Processor may condition the conduct of such inspection on the prior notification by Controller (at least ten calendar days in advance) and on the signing of a non-disclosure

agreement. Should there be a competitive relationship between the Processor and an inspector engaged by Controller, the Processor may reject the involvement of the respective inspector.

(3) In the event of a personal data breach by Processor, an inspection related to such breach may be carried out on reasonable short notice (i.e., after less than ten calendar days' prior notice). Any disturbances of the operating procedures shall be avoided to the greatest extent, nonetheless.

(4) Paragraph (2) above of this Section 7 shall apply accordingly to inspections carried out by a data protection authority or any other competent supervisory authority of Controller. The signing of a non-disclosure agreement is expendable, if and to the extent the respective authority is under an appropriate statutory obligation of confidentiality.

(5) Evidence of such measures, which concern not only the specific order, may also be provided by

- compliance with approved codes of conduct pursuant to Article 40 GDPR;
- certification according to an approved certification procedure in accordance with Article 42 GDPR;
- current 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.

8. Notification and supporting obligations of Processor

The Processor shall assist the Controller in complying with the obligations referred to in Articles 33 to 36 of the GDPR. Such assistance includes, in particular, without limitation:

- the immediate notification to Controller of any personal data breach;
- supporting the Controller with regard to Controller's obligation to provide information to the data subject. In this regard, the Processor will immediately provide the Controller with all relevant information;
- supporting the Controller with its data protection impact assessment;
- supporting the Controller with regard to prior consultation of the supervisory authority.

9. Authority of Controller to issue instructions; notification obligation of Controller

(1) The Controller shall immediately confirm oral instructions (at the minimum in text form).

(2) The Processor shall inform the Controller immediately if he considers that an instruction violates data protection regulations. The Processor shall then be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

(3) The Controller shall inform the Processor immediately if he notices mistakes or irregularities with regard to data protection regulations in Processor's outputs or work results.

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 or expiration of the Individual Order, the Processor shall hand over to the Controller or – subject to prior consent – destroy all documents and data sets related to the contract that have come into its possession, in a data protection compliant manner. 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 shall be stored beyond the contract duration by the Processor in accordance with the respective

retention periods. The Processor may hand such documentation over to the Controller at the end of the contract duration to relieve the Processor of this contractual obligation.

11. Allocation of costs

(1) In case that, on instructions from Controller, the Processor (i) assists the Controller in complying with the obligations referred to in Articles 33 to 36 of the GDPR (cf. Section 8 above) or (ii) provides services according to Section 4 above, Processor may claim remuneration, based on its then current hourly rates for consulting and support services. This shall not apply, however, if and to the extent the respective assistance/services are attributable to a breach of contract by Processor.

(2) In case of inspections at the Processor's business premises (cf. Section 7 above), Processor may claim remuneration for its efforts to enable the inspections and/or to support the conduct of the inspections, if and to the extent the inspections require efforts of more than one man-day per calendar year. The Processor's then current hourly rates for consulting and support services shall apply.

12. Final provisions

(1) If and to the extent there are Individual Orders in place between the Parties, which do not comprise an agreement on data processing in accordance with the GDPR, the regulations of this DPA shall apply accordingly to these Individual Orders.

(2) The regulations of this DPA shall apply accordingly to any future Individual Orders between the Parties regarding the provision of services by Processor to Controller, if not provided otherwise in the respective future Individual Order.

(3) Should a provision of this DPA be or become invalid or unenforceable or should there be a gap in this DPA, the effectiveness of the remaining provisions of this DPA shall not be affected. The parties shall replace the invalid or unenforceable provision or fill the gap, as applicable, by such valid and enforceable provision as comes closest to the economic purpose of this DPA.

(4) In the event of any conflict or inconsistency between the regulations of this DPA and the regulations of other parts of the Individual Order, the regulations of this DPA shall prevail.

(5) Modifications and amendments of this DPA require an agreement in writing or in text form, including an explicit reference to this DPA. The same applies to the waiver of this formal requirement.

Annex Technical and organizational measures pursuant to Article 32 GDPR

retarus

Annex

to Appendix “Data processing agreement (“DPA”) pursuant to Article 28 GDPR”

Technical and organizational measures pursuant to Article 32 GDPR

Status of document: V3.1 of 18 February 2021

The following package of measures encompasses the individual technical and organizational measures pursuant to Art. 32 GDPR to be implemented by the Processor in the course of its activity on the Controller’s behalf.

The statements on the data center relate to the Retarus headquarters at Aschauer Str. 30, Munich. They are intended as an example to be applied to all Processor data centers and apply as standard for any future Processor data centers.

This document contains the following sections:

I. Confidentiality (Art. 32 (1) (b) GDPR)

1. Physical access control

Measures as a protection against unauthorized access to data processing systems.

1.1 Property protection (data center)

a) Separate security zone, access to data center secured by access control system with chip cards
b) Door security (magnetic locks, badge readers and access logging)
c) CCTV with 24 hour recording
d) Burglar alarm system – see Section I.1.7 below
e) No external windows in the data center
f) Service shafts secured (air conditioning, ventilation, lifts etc.)
g) Emergency exits are secured against misuse – alarm triggered by escape door control units in basement

1.2 Property protection (building and offices)

a) Access to offices by access control system with chip cards
b) Door security (motor locks, badge readers and access logging)
c) CCTV of entrance doors after office hours
d) Protection of building exterior by motion sensors in staircase area

1.3 Security zones

a) Data center is a separate area with strict physical access restrictions and surveillance
b) The departments in charge of the administration of services, such as “Operation”, “Network” and “Application Management”, are grouped together, kept separate and equipped with an additional access control

1.4 Organizational access control

a) Inspections by security service after office hours
b) Regulations governing the use of keys
c) Regulations governing the locking of doors (doors and windows must be kept closed at all times, alarm system in data center armed in case of absence)
d) Marking of emergency exits and escape routes

1.5 Regulations regarding physical access authorization

(Relating to the data center)

a) Physical access regulations for persons and groups of people (employees, managers, third parties, visitors, servicing and cleaning personnel, suppliers, delivery companies etc.)
b) Regulations governing authorized personnel leaving the company and changes in authorization
c) Regulations / follow-up measures relating to the loss of badges, keys etc.
d) Regulations governing visitors incl. obligation to comply with data protection upon access
e) Registration and accompaniment of visitors and third parties
f) Supervision of servicing, maintenance and cleaning personnel
g) Ability to revise the allocation and revocation of physical access authorization

1.6 Personnel checks

a) Operating personnel control
b) Service, maintenance and cleaning personnel control
c) Visitor control

1.7 Alarm systems

a) Hazard detection system certified by the VdS
b) Disarming only possible for authorized personnel with chip card and additional code entry
c) Disarming ("forgotten" arming) outside core hours triggers an alarm in the permanently manned security guards office
d) Alarm in case of “door open“ longer than 30 seconds
e) Monitoring of data center by means of motion sensors
f) Duration until security team is on site: approximately 10 minutes
g) Detection lines for sabotage alarm, malfunctions etc. as standard
h) Maintenance contract in place

2. Access control

Measures to prevent unauthorized system access.

2.1 Regulation of access rights

(related to complete systems or individual applications)

a) Processes governing the allocation and management of access authorizations under redundant supervision (principle of multiple-assessor verification)
b) Regular checks on the validity of access authorization
c) Authorized persons are required to identify themselves by user ID and password
d) Password management for emergency users (administrator, root, etc.)
e) Password policy in place governing the use of passwords
f) Computers must be locked at all times in case of absence from the workplace
g) Limited authorization (account activation) for temporary employees / third parties
h) Regulations and defined procedures for company leavers and changing authorizations
i) Regulations in case of loss (forgetting) of the password(s)
j) Limitation of logon attempts
k) Disconnection in case of repeated failed attempts or timeouts

2.2 Network security

a) Separated networks for Services, internal/office use and visitors
b) Implementation of network security mechanisms (network access control via 802.1x or MAC filters) that prevent unauthorized access to the network.
c) Network protection through firewalls and virus scanners
d) Use of Intrusion Prevention Systems (IPS) and protection against DDOS attacks
e) Regular control of configurations and adjustment against specifications for the hardening of systems
f) Regulations for the release of new devices before commissioning in productive environments

2.3 Additional measures for remote access

a) Regulation governing the use of the remote connection, particularly for third parties
b) Only defined personnel will be permitted to log in remotely
c) Network access protection by hardware and software measures; e.g. access exclusively possible via VPN with 2-factor authentication
d) Regulations governing remote administration and maintenance (remote maintenance concept)
e) Regulations governing the remote access available to business partners (extranet)
f) Prevention of unauthorized access from the Internet (firewall)

2.4 Access logging

a) Evidence of the use of data processing systems (access logging)
b) Logging of failed login attempts (unblocking users)
c) Logging of allocations/changes of access authorizations

3. Data access control

Measures against unauthorized reading, copying, alteration or removal of personal data within the Retarus System.

3.1 Authorization concept

a) Regulations governing the allocation and management of access authorizations
b) Service-related definition of authorization management regulation for the input, information, modification and deletion of stored data (level of detail, assignment practice, signature authorization)
c) Individual access rights – creation of user groups
d) Guidelines for data management (e.g. expiry dates, retention periods, protection categories)

3.2 Access protection

a) Password-protected files
b) Separation of testing and production operations
c) Network access protection
d) Restricted authorizations for the use of utility programs or features that are appropriate to circumvent security measures
e) Limitation of unrestricted SQL query options of databases
f) Implementation of the erasure strategies through automated erasure of data in accordance with the respective retention periods.

3.3 Handling procedure for data storage devices

(Relating to the data center)

a) Regulation governing the applicable location/zone of specific data carriers
b) Zones are secured by access control system
c) Regulation on secure data carrier storage depending on the type of data carrier (blank/new, recorded, etc.)
d) Organizational regulations for data carrier storage (storage periods, clear identification of data carriers)
e) Determination of authorized persons for the removal of data media (key management/acknowledgement, return)
f) Generally no repair of data carriers, but disposal in accordance with data protection requirements (with confirmation of destruction and proof of disposal)
g) Regulations governing the production/distribution of copies and duplicates (archives inside and outside the company, printed matter etc.)
h) Regulation regarding the destruction of data carriers depending on the type of data carriers (HDD, magnetic tapes, flash memory etc.)

3.4 Access logging

In addition to the measures pursuant to Sect. II.2. the following applies:

a) Logging of read accesses
b) Logging of allocations/modifications of access authorizations

4. Separation control

Measures for the separate processing of personal data collected for different purposes.

4.1 Client segregation

a) Logical data segregation
b) Multi-client capability of applications
c) Authorization concept considers the assignment of rights for different purposes
d) Separated systems for production, testing and development
e) Restrictive use of SQL

4.2 Further organizational measures

a) Internal guidelines for data collection and processing
b) Documentation of database(s)
c) Documentation of processing programs
d) Documentation of data collection purposes
e) No integrated data storage

5. Encryption

Personal data processing measures in order to ensure that data cannot be attributed to a specific data subject without the use of additional information.

5.1 Use of encryption

a) Use of encryption routines (data carrier or file encryption) according to the risk classification
b) Encryption of passwords
c) Encrypted transmission of data from or to external networks using suitable transport protocols (SSL/TLS, SSH, S/MIME, PGP, etc.)

II. Integrity (Art. 32 (1) (b) GDPR)

1. Transfer control

Measures to prevent the unauthorized reading, copying, alteration or removal of personal data during electronic transmission or transport.

1.1 Electronic transmission control

a) Encrypted transmission of data from or to external networks using suitable transport protocols (SSL/TLS, SSH, S/MIME, PGP, etc.)
b) Email authentication (digital signature)
c) Determination of the points (third parties) to which data may be transmitted by data transmission facilities
d) Determination of authorized persons for the data transmission (authorization concept)
e) Documentation of the points to which transmission is intended as well as the transmission channels
f) Documentation of the download and transmission programs (e.g. FTP = File Transfer Protocol, Firewall, Remote Access)
g) Logging of data transmission and recipients

1.2 Handling of data carriers

In addition to the stipulations pursuant to Sect. I.3.3 the following applies:

a) Personal data will not be stored on removable media
b) Transport of data carriers with personal data is not provided for

2. Input control

Measures to determine whether and by whom personal data has been entered, modified or removed in data processing systems.

2.1 Monitoring and evaluation

a) Definition of responsibilities for data input (including substitution arrangements)
b) Logging of all entries, changes or deletions of personal data
c) Implementation of the principle of dual control
d) Differentiated user roles (e.g. read, write, change/delete)

III. Availability and capacity (Art. 32 (1) (b) GDPR)

1. Availability control

Protective measures against accidental or willful destruction or loss of personal data.

1.1 Creation and storage of backup copies

a) General backup concept
b) Regular backup of user files and databases
c) Name conventions for backup files
d) Labelling of data carriers
e) Use of write-protection on data storage devices
f) Inventory of backup copies (files, data carriers)
g) Archiving regulations
h) Inventory control of data carriers
i) Logging of security backups
j) Storage in highly protected areas
k) Definition of retention periods

1.2 Ensuring continuous operations

a) Power supply:

- Uninterruptible power supply through two UPS systems for the data center and emergency work stations
- Emergency power generator with sufficient fuel supply
- UPS for the NOC with sufficient capacity (UPS bridging up to 1 hour)
- Regular tests of the emergency power supply (load and open circuit tests)
- Maintenance contracts in place

b) Fire protection:

- N2 extinguishing system in the data center made by Total Walther. Certified by the VdS, approved pursuant to SprüfV (Safety Equipment Inspection Order)
- Connection to the building‘s central fire detection unit with alarm forwarding to the municipal fire brigade Munich
- In addition, connection to the alarm system when triggered (gas flow meter in the pipe system) with forwarding to the permanently manned security guards office
- Responsible Retarus employees (operating, IT management, technology management) will be notified by security service if alarm is triggered
- Optical and acoustic warnings in the data center in the event of a triggered alarm
- Operating panel of the Retarus central fire detection unit is being checked several times a day
- Maintenance contracts in place

c) Air conditioning:

- Two separate air conditioning systems of different technical designs and with separate routings
- Nine indoor units for optimized cooling distribution
- Leakage warning with forwarding to the permanently manned security guard office
- Responsible Retarus personnel (operating, IT management, technology management) will be notified by security service if alarm is triggered

- Temperature monitoring at several points, integration into the Retarus operating and incident management systems
- Maintenance contracts in place

d) IP-Connection:

- Redundant internet connection with separate routing and building connection/lead-in
- Direct connection to provider's fiber glass city ring. 24x7x365 service agreement

e) Telephone Backbone connection:

- Backbone connection to at least two carriers
- Constant load balancing
- 24x7x365 service agreement

f) Monitoring:

- 24x7 monitoring of IT Systems
- On-call services for interference elimination

g) Redundancies:

- High availability through cluster operation of key systems (network, server, peripherals)
- Provision of hardware replacements

1.3 Measures for emergency and disaster control

a) Emergency plan in the case of disasters (incl. responsibilities, recovery policy, on-call service, alternative data center premises etc.).
b) Business-Continuity-Policy (BCM)
c) Disaster-Recovery-Policy (DR)
d) Pandemic Preparedness Plan (PPP)
e) Protection against water influx/flooding
f) Regular testing of the components of the concepts

1.4 Organizational measures

a) Functional segregation of respective departments and IT unit
b) Staff substitution policies
c) Central and uniform procurement of hardware and software
d) Formalized approval process for new data processing methods and material changes to existing processes
e) Use of tested and approved third-party software only
f) Guidelines for process and program documentation
g) Issuance of instructions and safety guidelines
h) Appropriate user training
i) Appointment of a security officer
j) maintenance contracts and SLA's when using service providers
k) provision of network schematics

1.5 Further technical measures

a) Distribution of IT services across multiple systems
b) Central asset management of all components (CMDB)

IV. Procedures for regular review, assessment and evaluation (Art. 32 (1) (d) GDPR; Art. 25 (1) GDPR)

1. Order control

No order processing within the meaning of Art. 28 GDPR without corresponding instructions from the Controller.

1.1 Contractual arrangements

a) There is a written or at least electronic agreement (text form) in place for order processing between the Controller and the Processor.
b) Controller's instructions to the Processor shall be issued at least in text form; any verbal instructions shall be confirmed promptly at least in text form.
c) Processor shall have sufficient internal instructions relating to the order and the corresponding instructions of the Controller.

1.2 Subcontracting

a) Sufficient measures to ensure compliance with data protection laws by potential subcontractors may also be examined by the Controller.

1.3 Supervisory authorities

a) If the Processor has been inspected by a supervisory authority, the Controller may request the audit report. The same applies to inspections of potential subcontractors.

2. Management-Systems

2.1 Data protection management

a) Appointed data protection officer
b) Employees committed to data protection by written obligation
c) Operation of an information security management system (ISMS)

2.2 Incident-Response-Management

a) Regulations for the handling of data protection and security incidents
b) Regulations for inquiries from affected parties/data subjects

2.3 Change management

a) Changes to systems are subject to the central change management process
b) Implementation of a multi-eye principle for changes (Change Advisory Board)

2.4 Patch management

a) Regular updates of operating systems and applications
b) Automated routines for detecting patch requirements and performing updates

2.5 Regular review

a) Regular internal reviews and audits by IT compliance department
b) Regular vulnerability scans (vulnerability monitoring)
c) Regular external PEN tests to verify network and application security
d) Annual external audits of the internal control system in accordance with ISAE 3402 (SOC1) and ISAE 3000 (SOC2)

V. List of Changes

Version	Date	Changes	Editor
V3.0	07 March 2018	Redesign of the document due to implementation GDPR, all previous changes were deleted from the history	Philipp Deml
V3.1	18 February 2021	Revision and slight changes to the formatting Expansion of the catalog of measures Chapter I: 1.5 d), 2.1 a), 2.2 b), 3.2 f) Chapter III: 1.2 f) g), 1.3 d), 1.4 b) j) k), 1.5 Chapter IV: 2.3, 2.4, 2.5	Philipp Deml