Acuerdo Complementario

Tratamiento según el Art. 28 RGPD

Preámbulo

Los Servicios prestados por Retarus (en adelante, el “Encargado del tratamiento“ o “Encargado”) en beneficio del Cliente (en adelante, el „Responsable del tratamiento” o “Responsable”) incluyen, entre otros, el procesamiento de datos personales. Las disposiciones de este Acuerdo Complementario se aplican al tratamiento de los datos personales por parte del Encargado de Tratamiento en el marco de la prestación de sus Servicios y, en esta medida, concretan las obligaciones legales de protección de datos de las partes. De forma complementaria se aplicarán las disposiciones del Acuerdo Individual.

1. Objeto y duración del encargo

(1) El objeto del encargo de tratamiento de datos es la prestación de los Servicios que se describen en el Acuerdo Individual.

(2) La duración de este encargo (vigencia) se corresponde con la vigencia del Acuerdo Individual.

2. Concreción del contenido del encargo

(1) Tipo y finalidad del tratamiento de datos previsto

El tipo y la finalidad de las tareas del Encargado del tratamiento consisten en la prestación de Servicios de comunicación según se describen con detalle en el Acuerdo Individual.

El tratamiento de datos acordado contractualmente tendrá lugar exclusivamente en un Estado miembro de la Unión Europea o en otro Estado firmante del Tratado sobre el Espacio Económico Europeo. Cualquier transferencia de datos personales a un país tercero requiere la previa aprobación del Responsable y solo se puede producir si se cumplen las condiciones especiales de los Arts. 44 ss. RGPD. El Responsable del tratamiento no puede denegar la autorización arbitrariamente.

(2) Tipo de datos

El objeto del tratamiento de datos personales son los siguientes tipos/categorías de datos:

[x] Datos personales maestros

[x] Datos de comunicación (por ejemplo teléfono, correo electrónico, fax)

[ ] Datos contractuales maestros

[ ] Datos sobre liquidación contractual y pagos

[ ] _____

(3) Categorías de personas afectadas

Las categorías de las personas afectadas por el tratamiento abarcan:

[x] Destinatarios y remitentes de mensajes dirigidos al Responsable del tratamiento o que éste emita

[x] Empleados / Interlocutores

[ ] Clientes

[ ] Proveedores

[ ] Gerencia

[ ] _____

3. Medidas técnicas y organizativas

(1) El Encargado del tratamiento adoptará medidas técnicas y organizativas en el sentido del Art. 32 RGPD para proteger adecuadamente los datos del Responsable y asegurar de forma duradera la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y Servicios del tratamiento (véanse los detalles en el anexo a este Acuerdo Complementario).

(2) Las medidas técnicas y organizativas están sujetas al avance y desarrollo de la técnica. En este sentido, el Encargado del tratamiento está autorizado para aplicar medidas alternativas adecuadas. En tal caso no se podrá reducir el grado de seguridad de las medidas establecidas. Las modificaciones sustanciales deberán documentarse.

4. Derechos de los interesados

(1) El Encargado del tratamiento no puede por iniciativa propia rectificar, suprimir o limitar el tratamiento de los datos que procese por encargo, sino solo por instrucción documentada del Responsable. Si una persona interesada se dirige directamente al Encargado del Tratamiento en el ejercicio de sus derechos de rectificación, supresión o limitación del tratamiento o solicita información, el Encargado remitirá esta solicitud de inmediato al Responsable del tratamiento.

(2) El Encargado del tratamiento apoyará de forma razonable al Responsable, de acuerdo con las instrucciones del mismo, en la aplicación de su política de borrado, así como en la gestión de las solicitudes de interesados en relación con sus derechos, por ejemplo el derecho al olvido, rectificación, portabilidad de datos e información.

5. Aseguramiento de la calidad y otras obligaciones del Encargado

El Encargado del tratamiento está obligado a cumplir los requisitos que figuran a continuación:

(1) Nombramiento de un delegado de protección de datos que ejerza su actividad según los Arts. 38 s. RGPD.

El Encargado ha nombrado un delegado de protección de datos con el que se puede contactar en el correo electrónico

dataprivacy@retarus.com

En la página del Encargado se encuentran más datos de contacto actualizados de fácil acceso.

(2) Control periódico de los procesos internos y de las medidas técnicas y organizativas según el artículo 3, para garantizar que el tratamiento se produce, dentro de su ámbito de responsabilidad, de acuerdo con los requisitos del derecho vigentes sobre protección de datos y que se garantiza la protección de los derechos de la persona interesada.

(3) El Encargado garantiza que los empleados que se ocupen del tratamiento de los datos del Responsable y otras personas que actúen por cuenta del Encargado tienen prohibido tratar los datos fuera de las instrucciones del Responsable del tratamiento. Además, el Encargado garantiza que las personas facultadas para el tratamiento de los datos personales han suscrito la obligación de confidencialidad o bien están sujetas a una obligación legal adecuada de confidencialidad.

(4) En caso de que los datos del Responsable que tiene el Encargado del tratamiento corran peligro por pignoración o incautación, por un proceso de insolvencia o conciliación o por otras incidencias o medidas de terceros, el Encargado debe informar de inmediato al Responsable al respecto. El Encargado informará de inmediato a todas las personas responsables en este contexto de que la titularidad de los datos corresponde exclusivamente al Responsable como „Responsable del tratamiento“ en el sentido del RGPD.

6. Subcontratación

(1) La subcontratación a los efectos de este artículo 6 se ha de entender como encargo de servicios que se refieran directamente a la prestación del Servicio principal. No forman parte de ello las prestaciones accesorias que utilice el Encargado, como por ejemplo los servicios de telecomunicaciones, los servicios de correos/trasporte, los servicios de mantenimiento y de soporte del usuario o las medidas para asegurar la confidencialidad, la disponibilidad, la integridad y la resiliencia del hardware y el software de instalaciones de tratamiento de datos. Sin embargo, el Encargado está obligado, para garantizar la protección y la seguridad de los datos del Responsable, a adoptar acuerdos adecuados y conformes con la ley, así como a adoptar medidas de control, también en el caso de servicios accesorios externalizados.

(2) El empleo de subcontratistas (otros encargados del tratamiento) solo es admisible si el Responsable lo ha autorizado previamente. El Responsable no puede denegar la autorización sin un motivo importante sobre protección de datos.

(3) La autorización del Responsable para hacer un encargo a un subcontratista se considera otorgada si el Encargado le ha notificado al Responsable el encargo previsto por escrito o en forma de texto y el Responsable no presenta objeción a dicho encargo por escrito o en forma de texto dentro de los 14 días naturales siguientes a la recepción de la notificación.

(4) Si el Responsable deniega la autorización de una subcontratación prevista por el Encargado sin un motivo legal importante sobre protección de datos, el Encargado queda facultado para resolver el Acuerdo Individual aplicando un plazo de preaviso adecuado. Si en el Acuerdo Individual se han acordado Servicios distintos que sean separables entre sí y que el Responsable pueda utilizar de forma independiente, el derecho de resolución solo se aplicará a las partes del Acuerdo Individual que estén afectadas por la denegación de la subcontratación.

(5) El plazo de preaviso adecuado para una resolución de conformidad con el párrafo (4) que antecede es de un máximo de seis (6) meses o de la vigencia residual del Acuerdo Individual, tomando en cada caso el periodo más corto.

(6) El Responsable del tratamiento autoriza en virtud de este contrato la subcontratación con el siguiente subcontratista:

- retarus GmbH, Aschauer Straße 30, 81549 Múnich, Alemania

En la medida en que los Servicios en el ámbito del EDI y/o del OCR estén cubiertos por el Acuerdo Individual:

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

En la medida en que los Servicios en el ámbito de la seguridad del correo electrónico (E-Mail Security) estén cubiertos por el Acuerdo Individual:

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

(7) Si el Encargado realiza encargos a subcontratistas, este impondrá sus obligaciones legales de protección de datos dimanantes de este Acuerdo Complementario al subcontratista mediante un acuerdo según el Art. 28 párrafo 2-4 RGPD.

7. Derechos de control del Responsable

(1) El Encargado justificará con medios adecuados al Responsable el cumplimiento de las obligaciones del Encargado establecidas en el Art. 28 RGPD, en especial mediante la puesta a disposición de la información necesaria en cada caso.

(2) Si en el caso concreto fuera necesario realizar inspecciones por parte del Responsable o de un inspector encargado por éste, se llevarán a cabo durante los horarios comerciales habituales sin perturbar el proceso empresarial, previo aviso con una antelación adecuada (al menos 10 días naturales). El Encargado puede hacer depender la realización de la inspección de un preaviso adecuado y de la firma de una declaración de confidencialidad. Si el inspector encargado por el Responsable estuviese en situación de competencia con el Encargado, al Encargado le asiste un derecho de objeción contra él.

(3) En caso infracción del Encargado, o de las personas empleadas por él en el marco del encargo, de la normativa sobre la protección de datos personales del Responsable o de las disposiciones estipuladas en el contrato, puede tener lugar una inspección al respecto con un preaviso razonable reducido (esto es, menos de diez días naturales). Sin embargo, también en este caso hay que evitar en lo posible perturbar el proceso empresarial del Encargado.

(4) Si una autoridad de vigilancia de la protección de datos u otra autoridad de vigilancia del Responsbale realizase una inspección, básicamente se aplicará el párrafo (2) como corresponda. No es necesaria la firma de una obligación de confidencialidad si esa autoridad de inspección está sujeta al secreto profesional o legal cuya infracción esté penada en el Código Penal.

(5) La justificación de esas medidas, que no solo afectan al encargo concreto, también se puede llevar a cabo mediante

- el cumplimiento de los códigos de conducta autorizados según el Art. 40 RGPD;
- la certificación mediante un procedimiento de certificación autorizado según el Art. 42 RGPD;
- certificados actuales, informes o extractos de informes de instancias independientes (por ejemplo auditor, delegado de protección de datos, departamento de seguridad IT, auditores de protección de datos, auditores de calidad), o bien
- una certificación adecuada mediante auditoría de seguridad IT o de protección de datos.

8. Obligaciones de notificación y apoyo del Encargado

El Encargado apoyará al Responsable en el cumplimiento de las obligaciones reseñadas en los artículos 33 a 36 RGPD. En especial forman parte de ellas:

- la notificación inmediata al Responsable de infracciones en la protección de datos personales;
- el apoyo del Responsable en el marco de su obligación de informar a los interesados. En este contexto, el Encargado pondrá de inmediato a disposición del Responsable toda la información relevante;
- el apoyo al Responsable en su estimación de las evaluaciones de impacto relativas a la protección de datos;
- el apoyo al Responsable en el marco de consultas previas a la autoridad de inspección.

9. Poder directivo y obligación de informar por parte del Responsable

(1) El Responsable del tratamiento debe confirmar de inmediato las instrucciones verbales (al menos en forma de texto).

(2) El Encargado debe informar de inmediato al Responsable en caso de que considere que una instrucción infringe normas sobre protección de datos. El Encargado está facultado para suspender la realización de dicha instrucción hasta que la persona autorizada del Responsable la confirme o la modifique.

(3) El Responsable debe informar al Encargado de inmediato y de forma íntegra cuando constate que en los resultados del encargo hay errores o irregularidades en cuanto a las disposiciones legales sobre protección de datos.

10. Borrado y devolución de datos personales

(1) No se harán copias o duplicados de los datos sin conocimiento del Responsable del tratamiento. Aquí quedan excluidas las copias de seguridad, siempre que sean necesarias para garantizar un tratamiento correcto de los datos, y los datos que sean necesarios para el cumplimiento de plazos legales de conservación.

(2) Tras finalizar los trabajos contractuales, o antes tras requerimiento del Responsable – a más tardar al finalizar el Acuerdo Individual –, el Encargado debe entregar todos los documentos que obren en su poder, así como los datos relacionados con el encargo de tratamiento de datos, al Responsable del tratamiento o, previa autorización del mismo, destruirlos según la normativa de protección de datos. A petición deberá presentar el acta de borrado.

(3) Los documentos que sirvan para justificar el correcto tratamiento de datos según el encargo los debe conservar el Encargado más allá de la fecha de finalización del contrato según los correspondientes plazos de conservación. El encargado podrá entregar tal documentación al Responsable al finalizar el contrato para relevarle en su obligación legal de conservación.

11. Asunción de costes

(1) Si el Encargado apoya al Responsable por instrucción de éste en el cumplimiento de las obligaciones mencionadas en los artículos 33 hasta 36 RGPD (véase el artículo 8 de este Acuerdo Complementario) o presta servicios según el artículo 4 de este Acuerdo Complementario, el Encargado podrá exigir una retribución sobre la base de las tarifas horarias vigentes en cada caso para servicios de asesoramiento y soporte. Esto no se aplica si los servicios correspondientes se han hecho necesarios debido a una infracción del Encargado de sus obligaciones contractuales.

(2) Por el apoyo en la realización de una inspección según el artículo 7 de este Acuerdo Complementario, el Encargado puede exigir una retribución según las trifas horarias vigentes en cada caso para servicios de asesoramiento y soporte, siempre que el apoyo requiera el empleo de más de un día/hombre por cada año natural.

12. Disposiciones finales

(1) Este Acuerdo Complementario sustituye todos los posibles acuerdos anteriores entre las partes en cuanto al objeto de este Acuerdo Complementario (tratamiento de datos).

(2) Las disposiciones de este Acuerdo Complementario también se aplican a todos los posibles contratos futuros sobre la prestación de Servicios por parte del Encargado para el Responsable, siempre que en el contrato correspondiente no se disponga expresamente lo contrario.

(3) Si alguna disposición de este Acuerdo Complementario no fuese o llegase a ser eficaz o realizable, o si este Acuerdo Complementario presentase alguna laguna, ello no afectará a la eficacia ni a la realizabilidad de las restantes disposiciones de este Acuerdo Complementario. En este caso, las partes se comprometen a acordar, en lugar de la disposición ineficaz o para llenar la laguna, la disposición eficaz y/o realizable que más se aproxime al objetivo económico de este Acuerdo Complementario.

(4) Todas las disposiciones del Acuerdo Individual conservan su validez siempre que no queden modificadas por las disposiciones de este Acuerdo Complementario.

(5) Las modificaciones y los complementos de este Acuerdo Complementario requieren un acuerdo por escrito que también se puede producir en un formato electrónico (forma de texto), y la referencia expresa

de que se trata de una modificación o un complemento de estas condiciones. Esto también se aplica a la renuncia a este requisito de forma.

Anexo Medidas técnicas y de organización según el Art. 32 RGPD

Anexo
Medidas técnicas y organizativas en el sentido del Art. 32 RGPD
("Technical and organizational measures pursuant to Art. 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 **Fehler! Verweisquelle konnte nicht gefunden werden.** 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. **Fehler! Verweisquelle konnte nicht gefunden werden.** 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