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

retarus

Annex

to Appendix "Data processing agreement (DPA) in accordance with Article 28 GDPR"

Technical and organisational measures

pursuant to Art. 32 GDPR

Status of the document: V4.0 as of 25.07.2025

Preamble

The following catalogue of measures describes the individual technical and organisational measures to be taken by the contractor within the scope of its activities for the client in accordance with Art. 32 GDPR.

The statements on the data centre refers to the current locations of data processing and is considered standard for all future facilities.

This document contains the following chapters:

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

1. Physical access control

Measures to protect against unauthorised access to data processing equipment.

1.1 Physical security of data centres

a) Selection of professional data centre operators with audited security measures in accordance with relevant standards such as ISO/IEC 27001, SOC1, etc.
b) Operation of the Retarus infrastructure in a separate, locked area (e.g. rack cage, etc.) with strict access control
c) Documented building security concept with defined security zones by the operator
d) Electronic access control system with access logging
e) Access via chip card in combination with biometric features (fingerprint or hand veins)
f) Mantraps when changing security zones
g) Comprehensive video surveillance with recordings stored for at least 90 days
h) Fencing around the premises
i) On-site security personnel available 24/7
j) Alarm system connected to security personnel

1.2 Physical security of office buildings

a) Documented building security concept with defined security zones
b) Electronic access control system with access logging
c) Access via chip card
d) Process for issuing access media and keys, including logging
e) Video surveillance of entrance doors outside business hours
f) Instructions for locking regulations

1.3 Organisational access control

a) Processes for issuing, managing, revoking and checking access authorisations
b) Regulations in the event of loss/theft of access media
c) Guidelines for visitors and non-employees (registration and escort)
d) Supervision of maintenance and cleaning staff
e) Careful selection of external personnel and issuance of access authorisations by name

2. Logical access control

Measures to prevent unauthorised system access.

2.1 Regulation of access rights

a) Processes for granting, managing, revoking and reviewing access authorisations
b) Regular review of access authorisations
c) Use of personalised user IDs
d) Central management of administrative emergency users (breaking glass)
e) Password policy governing the handling of passwords
f) Established processes for resetting passwords (loss or forgetting)
g) Automatic locking of the desktop when leaving the workstation
h) Limitation of incorrect login attempts with subsequent lockout if exceeded
i) Time limits for temporary access authorisations
j) Logging of access usage, including failed login attempts

2.2 Network security

a) Strict separation of networks and zones such as production, office and guests (DMZ, VLAN)
b) Securing access to networks (NAC via 802.1x, Enterprise WPA, Radius)
c) Protection of the network by firewalls, endpoint protection and intrusion prevention systems (IPS)
d) Specifications for hardening and commissioning network devices, including regular compliance checks
e) Regulations for remote administration and remote maintenance
f) Remote access exclusively via VPN with 2-factor authentication

3. Data access control

Measures against unauthorised reading, copying, modification or removal of personal data within the system.

3.1 Authorisation concept

a) Regulations for assignment, management, revocation and review of access authorisations
b) Service-related definition of authorisation management for entering, viewing, modifying and deleting stored data
c) Role-based assignment of authorisations
d) Logged assignment/change of access authorisations

3.2 Access protection

a) System-side separation of development, testing and production
b) Restrictive use of SQL
c) Restriction of permission to use auxiliary programs or functions that are capable of circumventing security measures
d) Regulations for data retention (retention periods, deletion, protection requirements)
e) Automated deletion in accordance with defined retention periods

3.3 Use and management of data carriers

a) Regulations for secure data carrier storage depending on the protection requirements
b) Determination of persons authorised to remove data carriers
c) Regulation of the production/issue of copies and duplicates
d) Processes for the secure destruction of data carriers depending on the level of protection required

4. Separation control

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

4.1 Client separation

a) Logical separation of clients and their respective data
b) Purpose limitation of data and authorisations

4.2 Further measures

a) Internal guidelines for the collection and processing of data
b) Functional separation of systems (development, testing, production)
c) Documentation of processing, systems and data collection purposes
d) No integrated data storage

5. Encryption

Measures for processing personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

5.1 General

a) Guidelines on the use of appropriate encryption routines in accordance with the level of protection required
b) Established processes for key management

5.2 Technical measures

a) State-of-the-art encryption using methods such as AES, RSA, Elliptic Curve (EC)
b) Use of modern hash functions for signatures such as SHA-256, SHA-3
c) Password storage using recognised hash methods (salted hash)
d) Encrypted data transmission to/from external networks using suitable transport protocols (TLS, SSH, S/MIME, PGP)
e) Encrypted data carriers in mobile devices
f) For long-term storage (archive) encryption at file level

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

1. Transfer control

Measures to prevent unauthorised reading, copying, modification or removal of personal data during electronic transmission or transport.

1.1 Security during data transmission

a) Encrypted data transmission to/from external networks using suitable transport protocols (TLS, SSH, S/MIME, PGP)
b) Use of electronic signatures (for emails)
c) Definition of transmission routes, protocols and data recipients
d) Logging of data transmission

1.2 Secure handling of data carriers

The provisions under sectionI.3.3 also apply here. In addition, the following applies:

a) Regulations for the secure transport of data carriers have been defined
b) Transport of data carriers containing personal data is not provided for
c) Established technical restrictions on the use of USB removable data carriers

2. Input control

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

2.1 Logging and access

a) Concept for logging user activities, technical system events, errors and security-related activities
b) Authorisation concept considers rights for different purposes (read, write, delete)
c) Use of individual user IDs
d) Central storage of relevant logs with special requirements for access rights

III. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

1. Availability control

Measures to protect against accidental or intentional destruction or loss of personal data.

1.1 Data backup

a) General concept and guidelines for data backup
b) At least daily encrypted backup of configuration data and databases
c) Labelling of data carriers during storage (archiving)
d) Inventory control of data carriers
e) Logging of data backups and restores
f) Storage of backups of critical systems in a different fire compartment or at a different location
g) Sufficient retention period for backup data
h) Regular integrity tests and restore tests of backups

1.2 Secure operation in data centres

a) Uninterruptible power supply

- Redundant UPS system with emergency power generator
- Emergency power system with sufficient fuel supply and SLA for fuel replenishment
- Regular maintenance and testing of the emergency power supply

b) Fire protection and fire prevention

- Fire alarm system with early fire detection
- Extinguishing by means of extinguishing gas system (e.g. inert, argon)
- Direct connection to the local fire brigade
- Fire protection sections with min. fire resistance class F90
- Regular maintenance of the entire system

c) Air conditioning

- Redundant air conditioning systems (CRAC)
- Separation of cold and warm areas
- Permanent temperature monitoring
- Regular maintenance of the entire system

d) Internet connection and telephony

- Multiple redundant and carrier-neutral Internet connection
- Direct access to all important carriers and redundant connection to all important peering points (CIX-enabled site)
- Connection of the Retarus network to at least two different carriers
- Own product-specific load distribution
- SLA with 24/7 service agreements
- Protective measures against DDoS attacks

1.3 Provision and operation by Retarus

a) Issuing and central management of security guidelines and service instructions (SOP)
b) Formalised approval procedures for commissioning and changes (change management)
c) Asset management of all components used (CMDB)
d) Central configuration management and use of tools for system orchestration
e) Permanent active monitoring of systems (24x7x365)
f) Retarus internal on-call service for troubleshooting
g) Redundancy through cluster operation of all relevant systems in accordance with risk assessment
h) Replacement devices for important systems in stock

1.4 Measures for emergency and disaster control

a) Documented emergency and disaster planning as part of business continuity management
b) Clear responsibilities for activating the emergency board
c) Existing guidelines for business continuity (BCM plan), disaster recovery (DR plan) and pandemic preparedness (PP plan)
d) Regular review and testing of emergency plans
e) Appropriate training of affected employees in the application of the emergency concept

1.5 Further measures

a) Substitution arrangements
b) Centralised and standardized procurement of hardware and software
c) Approval processes for third-party software
d) Maintenance contracts and SLAs when using service providers

IV. Procedures for regular review, assessment and evaluation (Art. 32 (1) lit. 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 between the controller and the processor for order processing
b) The controller shall issue the instructions to the processor at least in text form or confirm any verbal instructions immediately in text form
c) The processor has sufficient internal instructions based on the order and the associated instructions of the controller

1.2 Subcontracting

a) Sufficient measures to ensure data protection by a potential subcontractor can also be checked by the controller
b) List of service providers

1.3 Supervisory authorities

a) In the event of an audit of the processor by the supervisory authority, the controller may request the audit report
b) Point a) also applies to audits of potential subcontractors

2. Management systems

2.1 Data protection management

a) Documented processes for reporting data protection incidents and handling requests from data subjects
b) Process for reviewing new data processing procedures in accordance with data protection law
c) Appointed Data Protection Officer
d) Employee confidentiality and data protection obligations
e) Processing directory

2.2 Information security management

a) Operation of a certified information security management system (ISMS) in accordance with ISO/IEC 27001
b) Appointment of an Information Security Officer

2.3 Incident response management

a) Regulations for dealing with data protection and security incidents
b) Regulations for enquiries from affected parties

2.4 Change management

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

2.5 Patch management

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

2.6 Regular review

a) Annual external auditing of the internal control system and ISMS in accordance with ISAE 3402 (SOC1), ISAE 3000 (SOC2), ISO/IEC 27001 and other relevant certifications.
b) Regular internal reviews and audits by the IT Compliance department
c) Regular vulnerability scans (vulnerability monitoring)
d) Regular external PEN tests to check network and application security

2.7 Data protection-friendly default settings (Art. 25 (2) GDPR)

Appropriate default settings and measures ensure that personal data is only processed in accordance with the specific purpose for which it was collected. This applies to the amount of personal data collected, the extent of its processing, its storage period and its accessibility.

This is achieved through the following measures, among others:

a) Design of services according to the "deliver & delete" principle
b) Automatic deletion routines
c) Application of privacy-by-design principles

V. Change log

Version	Date	Change	Editor
V3.0	07	Document redesigned due to implementation of GDPR; all previous changes have been deleted from the history.	Philipp Deml
V3	18	Revision and minor changes to the formatting. Expansion of the catalogue 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
V.3.1	24	Review; no changes	Philipp Deml
V.3.1	22	Review; No changes	Philipp Deml
V.3.1	26	Review; No changes	Philipp Deml
V4.0	25	Outsourcing of data centre operations (colocation provider), revision and adaptation of the wording of all measures to reflect the state of the art, summarising or deleting relevant points. Addition of Chapter IV, 2.7, inclusion of ISO/IEC 27001 certification.	Philipp Deml