ACCORDO PER IL TRATTAMENTO DI DATI PERSONALI

*in esecuzione dell' art. 28 del Regolamento Europeo n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati - **GDPR**)*

Premesse

Nell'ambito dell'esecuzione, da parte di retarus (Italia) S.r.l. (di seguito, il "**Responsabile**") in favore del cliente (di seguito, il "**Titolare**"), delle prestazioni regolate nell'incarico specifico conferito dal Titolare al Responsabile (di seguito, l'"**Incarico Specifico**") rientrano, fra l'altro, attività che includono o implicano il trattamento di dati personali.

Le disposizioni del presente accordo (di seguito, l'"**Accordo per il Trattamento Dati**") disciplinano le attività di trattamento di dati personali svolte dal Responsabile su incarico del Titolare in esecuzione dell'Incarico Specifico e stabiliscono gli obblighi e le facoltà del Responsabile e del Titolare (di seguito, congiuntamente, le "**Parti**") in ordine alla protezione degli stessi, in conformità alla normativa applicabile.

Il presente Accordo integrativo costituisce parte integrante e sostanziale dell'Incarico Specifico.

1. Oggetto e durata

(1) Il presente allegato disciplina l'attività di trattamento di dati personali da parte del Responsabile con riferimento alle prestazioni di cui all'Incarico Specifico.

(2) La durata dell'incarico per il trattamento dei dati corrisponde alla durata dell'Incarico Specifico.

2. Contenuto e caratteristiche delle attività di trattamento del Responsabile

(1) Natura e finalità del trattamento

Le attività affidate al Responsabile che implicano il trattamento di dati personali consistono nella fornitura e gestione di servizi di comunicazione, come meglio descritti nell'Incarico Specifico.

Il Responsabile è obbligato ad eseguire le attività di trattamento di dati personali esclusivamente nel territorio di uno Stato membro dell'Unione Europea, oppure appartenente allo Spazio Economico Europeo (Trattato EEA). Ogni operazione di trattamento o di trasferimento di dati personali fuori dall'Unione Europea o dallo Spazio Economico Europeo è subordinata alla previa autorizzazione scritta del Titolare e, in ogni caso, può avere luogo solo se ricorrono i presupposti previsti dagli artt. 44 e seguenti del GDPR. L'autorizzazione del Titolare al trasferimento dei dati fuori dall'Unione Europea o fuori dallo Spazio Economico Europeo non dovrà essere ingiustificatamente negata o ritardata.

(2) Tipologia di dati personali

Sono oggetto di trattamento le seguenti categorie di dati personali:

☒ Dati anagrafici

☒ Dati relativi alle comunicazioni (telefono, e-mail, fax)

☐ Dati contenuti nei documenti contrattuali (ad es., offerte, materiale pubblicitario)

☐ Dati di fatturazione e pagamento

☐ _____

(3) Categorie di interessati

Sono interessati dalle attività trattamento di dati personali le seguenti categorie di soggetti:

☒ destinatari di messaggi e comunicazioni inviate dal Titolare e mittenti dei messaggi indirizzati al Titolare;

☒ operatori, impiegati o incaricati del Titolare

☐ Clienti;

☐ Fornitori;

☐ Membri di organi societari o aziendali

☐ Altro _____

3. Misure tecniche e organizzative

(1) Il Responsabile dovrà adottare e mettere in atto misure tecniche e organizzative adeguate ai sensi dell'art. 32 del GDPR al fine di garantire un'adeguata protezione dei dati personali trattati per conto del Titolare. In particolare, le misure tecniche e organizzative adottate dal Responsabile dovranno essere idonee ad assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi di protezione dei dati (le misure adottate dal Responsabile ai sensi dell'art. 32 GDPR sono elencate e descritte nel documento in appendice al presente Accordo per il Trattamento Dati).

(2) Il Responsabile dovrà aggiornare e sviluppare le misure di protezione dei dati personali di cui al presente articolo tenendo conto del contesto tecnologico esistente e dei suoi futuri cambiamenti. A questo fine, il Responsabile potrà modificare in ogni momento la tipologia o la natura delle misure di protezione dei dati personali, anche mediante l'adozione di misure nuove o alternative rispetto a quelle già adottate, sempre che ciò non comporti una diminuzione del livello di sicurezza relativo alla protezione dei dati. In ogni caso, ogni cambiamento sostanziale dovrà essere documentato.

4. Diritti degli interessati dal trattamento dei dati

(1) Il Responsabile non potrà limitare, modificare, rettificare o cancellare di sua iniziativa i dati personali trattati per conto del Titolare ma solo su istruzione documentata dello stesso. Qualora un interessato contattasse direttamente il Responsabile chiedendo la rettifica o la cancellazione dei dati o limitazioni del trattamento, oppure lo contatti per una richiesta di informazioni su queste tematiche, il Responsabile dovrà immediatamente inoltrare la comunicazione o la richiesta al Titolare.

(2) Il Responsabile, conformemente alle direttive fornite dal Titolare, dovrà assisterlo nell'implementazione di procedure per la cancellazione dei dati personali nonché per la gestione delle richieste degli interessati con riferimento all'esercizio dei propri diritti e facoltà di cui al Capo III del GDPR (ad esempio, diritto di accesso, rettifica, cancellazione e portabilità dei dati).

5. Standard qualitativi nell'esecuzione dei servizi e altri obblighi del Responsabile

Al fine di assicurare un elevato standard di qualità nell'erogazione dei servizi, il Responsabile è tenuto a:

(1) Nominare un Responsabile per la Protezione dei Dati ai sensi degli artt. 37 e seguenti del GDPR:

A questo proposito, si dà atto sin d'ora che il Responsabile ha già provveduto alla nomina di un Responsabile per la Protezione dei Dati che potrà essere contattato al seguente indirizzo e-mail:

dataprivacy@retarus.com

Ulteriori informazioni di contatto possono essere consultate sul sito web del Responsabile.

(2) Monitorare periodicamente le proprie procedure interne e l'applicazione delle misure tecniche e organizzative di cui al precedente art. 3 al fine di assicurare che le operazioni di trattamento eseguite sotto la propria responsabilità siano conformi alla normativa in materia di protezione dei dati personali, con particolare riferimento alla protezione dei diritti degli interessati.

(3) Fare in modo che (i) i propri dipendenti o incaricati a cui sono affidate le operazioni di trattamento e (ii) ogni altra persona che, allo stesso fine, agisca su suo incarico, svolgano le operazioni di trattamento in conformità alle istruzioni fornite dal Titolare. Inoltre, il Responsabile garantisce che il personale autorizzato al trattamento dei dati si sia impegnato a mantenere riservate le informazioni apprese, o comunque sia vincolato per legge all'obbligo di riservatezza con riferimento alle attività di trattamento.

(4) Informare immediatamente il Titolare nel caso in cui vi fosse pericolo di perdita dei dati personali a causa di provvedimenti di confisca/sequestro, di procedure di insolvenza o di altri eventi esterni o riconducibili all'intervento di terzi. In tali casi, per impedire o limitare la perdita dei dati, il Responsabile dovrà informare senza ritardo tutte le persone, gli organi o le autorità che, a vario titolo, sono coinvolti nell'eventuale procedura di sequestro/confisca, insolvenza o altro, che i dati personali appartengono esclusivamente al Titolare in qualità di titolare del trattamento dei dati ai sensi del GDPR.

6. Sub-affidamenti

(1) Ai fini del presente articolo, per "sub-affidamento" deve intendersi l'affidamento a terzi, da parte del Responsabile, di prestazioni direttamente correlate all'esecuzione dell'Incarico Specifico. Devono intendersi escluse, pertanto, tutte le attività accessorie, tra cui, in particolare, servizi di telecomunicazione, servizi postali, di trasporto, manutenzione e supporto all'utente, come anche le misure per garantire la riservatezza, la disponibilità, l'integrità e la resilienza delle infrastrutture fisiche o virtuali impiegati nelle operazioni di trattamento. Il Responsabile sarà obbligato, in ogni caso, mediante stipula di idonei accordi giuridicamente vincolanti e mediante apposite verifiche, a garantire la protezione e la sicurezza dei dati forniti dal Titolare anche in caso di sub-affidamento di servizi o attività accessorie.

(2) Il Responsabile potrà ricorrere ad altri sub-responsabili soltanto previa autorizzazione scritta, generale o specifica, del Titolare ai sensi dell'art. 28 co. 2 GDPR. Il Titolare potrà negare l'autorizzazione solo per giustificati motivi inerenti l'applicazione della normativa in materia di protezione dei dati personali.

(3) L'autorizzazione del Titolare per il ricorso ad altri sub-responsabili s'intenderà automaticamente rilasciata al Responsabile se (i) Il Responsabile ha informato il Titolare in forma scritta, o altra forma equivalente, della propria intenzione di avvalersi di un determinato sub-responsabile e (ii) il Titolare non ha espresso il suo rifiuto in forma scritta, o altra forma equivalente, nel termine di 14 giorni di calendario dal ricevimento dell'informativa.

(4) Nel caso in cui il Titolare negasse al Responsabile l'autorizzazione ad avvalersi di sub-responsabili senza alcuna valida motivazione correlata alla normativa in materia di protezione dei dati personali, il Responsabile potrà recedere dall'Incarico Specifico, con un congruo preavviso. Se l'Incarico Specifico comprende diverse prestazioni, indipendenti l'una dall'altra e che possono essere autonomamente fruite ed utilizzate dal Titolare, il recesso avrà efficacia solo con riferimento a quelle prestazioni dell'Incarico Specifico per le quali Titolare ha negato al responsabile l'autorizzazione ad avvalersi dell'attività di altri sub-responsabili.

(5) La durata massima del preavviso di cui al precedente punto 4 è pari a 6 mesi o al residuo termine di durata dell'Incarico Specifico, se inferiore.

(6) Il Titolare autorizza sin d'ora il Responsabile ad avvalersi del seguente-sub-responsabile:

- retarus GmbH, Aschauer Straße 30, 81549 Monaco di Baviera, Germania

Nella misura in cui i servizi nell'area EDI e/o OCR sono oggetto dell'Incarico Specifico:

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

Nella misura in cui i servizi nell'area sicurezza della posta elettronica (E-Mail Security) sono oggetto dell'Incarico Specifico:

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

(7) In caso di sub-affidamento, il Responsabile è tenuto a stipulare con il sub-responsabile un contratto o un altro atto giuridico che obblighi quest'ultimo al rispetto degli stessi obblighi previsti a carico del Responsabile dal presente Accordo per il Trattamento Dati, in conformità a quanto previsto dall'art. 28 GDPR.

7. Poteri di supervisione e controllo del Titolare

(1) Il Responsabile è tenuto a documentare e comprovare la conformità del suo operato con gli obblighi previsti a suo carico dall'art. 28 GDPR, nei modi e nelle forme più opportune, e in particolare, fra l'altro, mettendo sempre a disposizione tutte le informazioni di volta in volta necessarie.

(2) Qualora, in un determinato caso, fosse necessario eseguire un'ispezione presso i locali commerciali del Responsabile, la stessa sarà condotta – dal Titolare o da suoi incaricati – con almeno 10 giorni di calendario di preavviso, durante il normale orario di lavoro e senza disturbare l'attività in corso. In tali casi, il Responsabile avrà facoltà di condizionare l'esecuzione dell'ispezione al ricevimento del preavviso (di almeno 10 giorni) e alla sottoscrizione, con il Titolare, di un accordo di riservatezza. Qualora l'ispezione fosse affidata dal Titolare a propri incaricati che si trovano in rapporto o in situazioni di concorrenza commerciale con il Responsabile, questi potrà opporsi al loro coinvolgimento nel processo di ispezione.

(3) In caso di violazione della normativa in materia di protezione dei dati personali da parte del Responsabile o da parte di propri incaricati che agiscono nell'ambito delle attività di trattamento di cui al presente Accordo per il Trattamento Dati, l'ispezione relativa alla violazione potrà essere eseguita con un preavviso ragionevolmente breve (vale a dire, anche minore di dieci giorni). In ogni caso, dovrà essere evitata o comunque ridotta al minimo indispensabile ogni interferenza con le attività lavorative in corso presso i locali interessati dall'ispezione.

(4) Quanto previsto al precedente punto (2) di questo articolo si applicherà, in linea di principio, anche nei casi di ispezioni condotte dalle autorità competenti in materia di protezione dei dati personali e ai controlli eseguiti da ogni altra autorità competente a vigilare sull'attività del Titolare. In tali casi, non è obbligatoria la sottoscrizione di un accordo di riservatezza, se e nella misura in cui l'autorità che esegue il controllo è giuridicamente vincolata a non divulgare le informazioni apprese nell'ambito della propria attività in base ad una specifica disposizione di legge.

(5) Il Responsabile potrà dimostrare la propria conformità agli obblighi previsti dall'art. 28 GDPR - in particolare per ciò che concerne l'adozione di adeguate misure tecniche e organizzative di protezione dei dati nel contesto della propria complessiva attività imprenditoriale - anche attraverso i seguenti adempimenti:

- l'adesione ad un codice di condotta approvato ai sensi dell'art. 40 GDPR;
- l'adesione ad un meccanismo di certificazione di cui all'art. 42 GDPR;
- il possesso attuale di certificati e attestati conseguiti in esito ad una procedura di revisione interna ("audit") o di rapporti compilati da soggetti indipendenti (ad esempio, revisori esterni, Responsabili per la protezione dei dati, responsabili della sicurezza informatica, responsabili del controllo qualità);
- il possesso di un'adeguata certificazione ottenuta in base ad un processo di revisione e controllo delle misure di sicurezza informatica e di protezione dei dati personali.

8. Obblighi di comunicazione e di assistenza del Responsabile

Il Responsabile dovrà assistere il Titolare nell'adempimento degli obblighi previsti a carico di quest'ultimo agli artt. 33-36 GDPR. In particolare, i compiti di assistenza del Responsabile consistono nelle seguenti attività:

- comunicare senza ritardo al Titolare ogni violazione dei dati personali;
- assistere il Titolare con riferimento ai suoi obblighi nei confronti dei soggetti interessati dal trattamento dei dati ai sensi dell'art. 28 co. 2, l. e) GDPR; in questi casi, il Responsabile dovrà tempestivamente mettere a disposizione del Titolare tutte le informazioni rilevanti;
- assistere il Titolare nella valutazione d'impatto del trattamento sulla protezione dei dati, con riferimento ai rischi di cui all'art. 35 GDPR;
- assistere il Titolare con riguardo alla consultazione preventiva dell'autorità di controllo nei casi previsti dal GDPR.

9. Poteri di istruzione del Titolare; obbligo di notifica del Titolare

(1) Il Titolare dovrà immediatamente confermare in forma scritta le istruzioni fornite oralmente al Responsabile.

(2) Il Responsabile dovrà immediatamente informare il Titolare se, a proprio giudizio, una sua istruzione viola la normativa in materia di protezione dei dati personali. Il Responsabile avrà inoltre la facoltà di sospendere l'esecuzione di un'istruzione del Titolare ritenuta contraria alla normativa applicabile, sino a che il Titolare non la confermi o la revochi.

(3) Il Titolare dovrà immediatamente informare il Responsabile nel caso in cui rilevi irregolarità o violazioni della normativa in materia di protezione dei dati personali nell'esecuzione dei compiti ad esso affidati.

10. Cancellazione e restituzione dei dati

(1) Il Responsabile non potrà creare copie o duplicati dei dati trattati senza che ne sia informato il Titolare, ad eccezione delle copie di sicurezza necessarie ad assicurare il regolare processo di trattamento, nonché ad eccezione delle ipotesi in cui sia necessario al fine di rispettare gli obblighi di legge relativi alla conservazione dei dati.

(2) Dopo la conclusione delle attività affidate, o anche prima se richiesto dal Titolare, e comunque, al più tardi, dopo lo scioglimento o la cessazione dell'Incarico Specifico, il Responsabile dovrà restituire oppure dovrà distruggere tutti i documenti e i dati relativi all'Incarico Specifico in suo possesso, conformemente a quanto previsto dalla normativa applicabile. Se si tratta di documenti informatici, il Responsabile dovrà fornire al Titolare, se richiesto, le prove dell'avvenuta distruzione/cancellazione.

(3) La documentazione utile a comprovare la regolarità delle operazioni di trattamento rispetto alle istruzioni ricevute dovrà essere conservata dal Responsabile anche oltre la durata del contratto, nel rispetto delle tempistiche di conservazione applicabili. Il Responsabile potrà consegnare tale documentazione al Titolare al termine del periodo di durata del contratto, al fine di liberarsi dai propri obblighi.

11. Costi e spese

(1) Nei casi in cui, su istruzione documentata del Titolare, il Responsabile: (i) assiste il Titolare nell'adempimento degli obblighi previsti agli art. 33-36 GDPR, come previsto al precedente art. 8, o (ii) fornisce assistenza al Titolare ai sensi di quanto previsto al precedente art. 4, avrà diritto ad un corrispettivo da quantificarsi in base alle sue tariffe orarie per i servizi di consulenza e assistenza. Tuttavia, al Responsabile non sarà dovuto alcun corrispettivo se le prestazioni di assistenza rese al Titolare sono imputabili ad una violazione del contratto da parte dello stesso Responsabile.

(2) In caso di ispezione presso i locali commerciali ai sensi del precedente art. 7, il Responsabile potrà chiedere una remunerazione/indennità per i disagi sopportati e/o per le attività di supporto e assistenza al Titolare, nei limiti in cui l'ispezione richieda l'impiego di più di un unità lavorativa al giorno per anno. Ai fini del calcolo della predetta remunerazione/ indennità si applicheranno i compensi orari del Responsabile per i servizi di consulenza e assistenza.

12. Disposizioni finali

(1) Qualora esistano già, fra le Parti, Incarichi Specifici aventi ad oggetto l'esecuzione di prestazioni da parte del Responsabile in favore del Titolare, i quali non contengano accordi specifici relativi al trattamento dei dati ai sensi del GDPR, le disposizioni del presente Accordo per il Trattamento Dati troveranno applicazione anche con riferimento a tali Incarichi Specifici.

(2) Le disposizioni del presente Accordo per il Trattamento Dati troveranno inoltre applicazione con riferimento a tutti i futuri accordi fra le Parti che abbiano per oggetto la fornitura di servizi da parte del Responsabile in favore del Titolare, salvo che non sia diversamente stabilito nel relativo contratto.

(3) Qualora una o più disposizioni del presente Accordo per il Trattamento Dati fossero dichiarate nulle o divenissero invalide o inapplicabili, o comunque nel caso di lacune o di inefficacia, anche sopravvenuta, di una o più parti dello stesso, le altre parti rimarranno valide fra le Parti ad ogni effetto. Le Parti, ove possibile, sostituiranno le previsioni nulle, inefficaci o inapplicabili con nuove disposizioni il cui contenuto dovrà essere il più possibile affine e compatibile con l'oggetto e le finalità economiche del presente Accordo per il Trattamento Dati.

(4) Qualora dovessero sussistere contrasti o incongruenze tra le disposizioni del presente Accordo per il Trattamento Dati e le disposizioni dell'Incarico Specifico, le disposizioni del presente Accordo per il Trattamento Dati prevarranno.

(5) Tutte le modifiche e le aggiunte al presente Accordo per il Trattamento Dati avranno efficacia solo se concordate tra le Parti in forma scritta che possono essere anche in formato elettronico (forma di testo), con espresso riferimento al presente Accordo per il Trattamento Dati. Anche la deroga o la rinuncia a quanto previsto dal presente articolo dovrà essere concordata in forma scritta.

Appendice Misure tecniche e organizzative ai sensi dell' art. 32 GDPR

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