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

Appendice

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

(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 I.1.7 below
e) No external windows in the data center
f) Service shafts secured (air conditioning, ventilation, lifts etc.)
g) Emergency exits are secured against misuse – alarm triggered by escape door control units in basement

1.2 Property protection (building and offices)

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

1.3 Security zones

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

1.4 Organizational access control

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

1.5 Regulations regarding physical access authorization

(Relating to the data center)

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

1.6 Personnel checks

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

1.7 Alarm systems

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

2. Access control

Measures to prevent unauthorized system access.

2.1 Regulation of access rights

(related to complete systems or individual applications)

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

2.2 Network security

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

2.3 Additional measures for remote access

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

2.4 Access logging

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

3. Data access control

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

3.1 Authorization concept

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

3.2 Access protection

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

3.3 Handling procedure for data storage devices

(Relating to the data center)

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

3.4 Access logging

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

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

4. Separation control

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

4.1 Client segregation

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

4.2 Further organizational measures

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

5. Encryption

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

5.1 Use of encryption

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

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

1. Transfer control

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

1.1 Electronic transmission control

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

1.2 Handling of data carriers

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

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

2. Input control

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

2.1 Monitoring and evaluation

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

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

1. Availability control

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

1.1 Creation and storage of backup copies

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

1.2 Ensuring continuous operations

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

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

c) Air conditioning:
- Two separate air conditioning systems of different technical designs and with separate routings
- Nine indoor units for optimized cooling distribution
- Leakage warning with forwarding to the permanently manned security guard office
- Responsible Retarus personnel (operating, IT management, technology management) will be notified by security service if alarm is triggered
- Temperature monitoring at several points, integration into the Retarus operating and incident management systems
- Maintenance contracts in place

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

e) Telephone Backbone connection:
- Backbone connection to at least two carriers
- Constant load balancing
- 24x7x365 service agreement

f) Monitoring:
- 24x7 monitoring of IT Systems
- On-call services for interference elimination

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

1.3 Measures for emergency and disaster control

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

1.4 Organizational measures

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

1.5 Further technical measures

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

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

1. Order control

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

1.1 Contractual arrangements

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

1.2 Subcontracting

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

1.3 Supervisory authorities

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

2. Management-Systems

2.1 Data protection management

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

2.2 Incident-Response-Management

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

2.3 Change management

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

2.4 Patch management

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

2.5 Regular review

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

V. List of Changes

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