retarus

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

Preamble

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

1. Subject matter and term of the order

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

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

2. Specification of order details

(1) Nature and purpose of the intended processing

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

The performance of the contractually agreed processing shall be carried out exclusively within a member state of the European Union (EU) or within a member state of the European Economic Area (EEA). Any transfer of personal data to a state which is not a member state of either the EU or the EEA requires the prior agreement of the Controller and shall only occur if the specific conditions of Articles 44 et seq. GDPR have been fulfilled. Controller’s agreement shall not be unreasonably withheld or delayed.

(2) Types of personal data

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

- ☒ Personal master data
- ☒ Communication data (e. g. telephone, e-mail, fax)
- ☐ Key contract data
- ☐ Contract billing and payments data
- ☐ _____

(3) Categories of data subjects

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

- ☒ Recipients and senders of messages addressed to or sent by Controller
- ☒ Controller’s employees / contact persons
- ☐ Customers
- ☐ Suppliers
- ☐ Board of managers
- ☐ _____

3. Technical and organisational measures

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

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

4. Data subjects' rights

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

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

5. Quality assurance and further obligations of Processor

The Processor shall meet the requirements as specified below:

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

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

dataprivacy@retarus.com

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

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

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

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

6. Subcontracting

(1) Subcontracting for the purpose of this Section 6 is to be understood as the commissioning of services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services as well as measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Processor shall, however, be obliged to make

appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Controller's data even in the case of outsourced ancillary services.

(2) The Processor may commission subcontractors (additional processors) only after prior consent from the Controller. Controller's consent may only be withheld for a compelling reason regarding data protection law.

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

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

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

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

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

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

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

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

7. Supervisory powers of Controller

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

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

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

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

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

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

- compliance with approved codes of conduct pursuant to Article 40 GDPR;
- certification according to an approved certification procedure in accordance with Article 42 GDPR;
- current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor); or
- a suitable certification by IT security or data protection auditing.

8. Notification and supporting obligations of Processor

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

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

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

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

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

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

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Controller, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Controller, at the latest upon termination or expiration of the Individual Order, the Processor shall hand over to the Controller or – subject to prior consent – destroy all documents and data sets related to the contract that have come into its possession, in a data protection compliant manner. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the order shall be stored beyond the contract duration by the Processor in accordance with the respective

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

11. Allocation of costs

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

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

12. Final provisions

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

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

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

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

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

Annex Technical and organizational measures pursuant to Article 32 GDPR

retarus

Annex

to Appendix "Data processing agreement (DPA) 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