

Data Processing Agreement

This Data Processing Agreement (“DPA”) applies between apsware GmbH, Am Hockeypark 10, 41179 Mönchengladbach, Germany (“apsware” or “Processor”), and the customer identified in the applicable agreement, order, statement of work or other contractual document referencing this DPA (“Customer” or “Controller”).

This DPA forms an integral part of the agreement, order, statement of work or other contractual document that references this DPA (the “Main Contract”). It applies to the extent that apsware processes Personal Data on behalf of the Customer in connection with the services provided under the Main Contract.

This DPA shall become effective on the effective date of the Main Contract or, if the Main Contract is already in force when reference to this DPA is made, on the date on which this DPA is incorporated into the Main Contract (“Effective Date”).

Preamble

The Parties enter into this DPA to ensure that the Processing of Personal Data by apsware on behalf of the Customer complies with the requirements of applicable Data Protection Laws, in particular Article 28 of Regulation (EU) 2016/679 (“GDPR”).

The Customer determines the purposes and means of the Processing of Personal Data and acts as the Controller. apsware processes Personal Data on behalf of the Customer and acts as the Processor.

This DPA sets out the Parties’ respective rights and obligations with regard to such Processing and supplements the Main Contract. Unless otherwise expressly provided in this DPA, the terms of the Main Contract remain unaffected.

Section I

Clause 1 (Purpose and Scope)

- a) This DPA governs the Processing of Personal Data by apsware on behalf of the Customer in connection with the services provided under the Main Contract and sets out the terms required pursuant to Article 28(3) of the GDPR.
- b) This DPA applies to all Processing activities performed by apsware in its capacity as Processor on behalf of the Customer under the Main Contract.
- c) This DPA does not apply to Processing activities for which apsware determines the purposes and means of Processing and therefore acts as an independent Controller.
- d) Any annexes or schedules to this DPA form an integral part of this DPA.
- e) Unless otherwise defined in this DPA, the terms “Personal Data”, “Processing”, “Controller”, “Processor”, “Data Subject” and “Personal Data Breach” shall have the meanings given to them in the GDPR.

Clause 2 (Incorporation and Relationship with the Main Contract)

- a) This DPA supplements and forms an integral part of the Main Contract.
- b) By entering into a Main Contract that references this DPA, the Parties agree to be bound by the terms of this DPA. A separate signature of this DPA is not required unless expressly agreed by the Parties or required by applicable law.
- c) In the event of any conflict between this DPA and the Main Contract with respect to the Processing or protection of Personal Data, this DPA shall prevail.

- d) All commercial terms, including the scope of the services, remuneration and general liability provisions, remain governed by the Main Contract unless expressly provided otherwise in this DPA.
- e) The version of this DPA in effect on the Effective Date shall apply to the relevant Main Contract. apsware may update this DPA from time to time. Unless otherwise agreed, any updated version shall apply to an existing Main Contract only where this is expressly agreed between the Parties or otherwise permitted under the Main Contract and applicable law.

Clause 3 (Interpretation)

- a) “Data Protection Laws” means the GDPR and any applicable national data protection laws supplementing or implementing the GDPR, in each case as amended from time to time.
- b) Capitalised terms relating to data protection that are not specifically defined in this DPA shall have the meanings given to them in the GDPR.
- c) References to Articles are references to Articles of the GDPR unless expressly stated otherwise.
- d) This DPA shall be interpreted in a manner consistent with the requirements of Article 28 GDPR and other applicable Data Protection Laws

Clause 4 (Term)

- a) This DPA shall commence on the Effective Date and shall remain in force for as long as apsware Processes Personal Data on behalf of the Customer under the Main Contract.
- b) The termination or expiry of the Main Contract shall not affect the application of this DPA for as long as apsware continues to Process Personal Data on behalf of the Customer, including for the purposes of returning or deleting Personal Data.
- c) Where applicable law requires apsware to retain Personal Data after termination of the Main Contract, apsware shall continue to protect such Personal Data in accordance with this DPA and shall Process it only to the extent required by applicable law.

Clause 5 (Customer Responsibilities)

- a) The Customer shall ensure that its Processing of Personal Data, including any instructions issued to apsware, complies with applicable Data Protection Laws.
- b) The Customer is responsible for ensuring that it has a valid legal basis for the Processing of Personal Data and for providing any information or notices to Data Subjects required under applicable Data Protection Laws.
- c) The Customer shall not instruct apsware to Process Personal Data in a manner that would violate applicable Data Protection Laws.
- d) The Customer shall provide apsware with all information reasonably necessary for apsware to perform its obligations under this DPA.

SECTION II – Obligations of the Parties

Clause 6 (Description of processing)

- a) The subject matter and purpose of the Processing are the Processing activities necessary for apsware to provide the services to the Customer under the Main Contract.
- b) The nature of the Processing, the categories of Data Subjects, the types of Personal Data

concerned and the duration of the Processing are described in Annex I to this DPA and, where applicable, further specified in the Main Contract.

- c) The specific scope of Processing may vary depending on the services ordered by the Customer under the Main Contract. Only those categories of Data Subjects, types of Personal Data and Processing activities that are relevant to the respective services shall apply.
- d) Any further or more specific Processing instructions issued by the Customer in accordance with Clause 7.1 shall form part of the description of Processing for the purposes of this DPA, provided that such instructions comply with applicable Data Protection Laws.

Clause 7 (Obligations of the Parties)

7.1 Instructions

- a) apsware shall Process Personal Data only on documented instructions from the Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless apsware is required to do so by Union or Member State law to which apsware is subject. In such a case, apsware shall inform the Customer of that legal requirement before Processing, unless the applicable law prohibits such information on important grounds of public interest.
- b) The Customer may issue further documented instructions throughout the duration of the Processing. Instructions may be provided in writing, including by email or other documented electronic means. In urgent cases, oral instructions may be given provided that they are confirmed in documented form without undue delay.
- c) apsware shall inform the Customer without undue delay if, in its opinion, an instruction infringes the GDPR or other applicable Data Protection Laws. apsware may suspend the execution of the relevant instruction until the Customer confirms, modifies or withdraws it.
- d) Persons authorised to issue instructions on behalf of the Customer shall be the persons designated by the Customer in the Main Contract or otherwise communicated to apsware in documented form. Instructions shall be addressed to the contact persons or communication channels designated by apsware for the relevant services.

7.2 Purpose limitation

apsware shall Process Personal Data only for the purposes described in Annex I, the Main Contract and any documented instructions of the Customer issued in accordance with this DPA.

7.3 Duration of processing of personal data

apsware shall Process Personal Data for the duration specified in Clause 4 and only for as long as necessary to provide the services under the Main Contract, unless applicable law requires longer retention.

7.4 Security of processing

- a) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risks to the rights and freedoms of natural persons, apsware shall implement and maintain appropriate technical and organisational measures in accordance with Article 32 GDPR.
- b) The technical and organisational measures implemented by apsware are described in Annex II. apsware may update or modify such measures from time to time, provided that the overall level of security is not materially reduced during the term of the Processing.

- c) apsware shall ensure that persons authorised to Process Personal Data have access to such Personal Data only to the extent necessary for the performance of their duties and are subject to appropriate confidentiality obligations.
- d) apsware shall maintain appropriate measures designed to ensure the confidentiality, integrity, availability and resilience of systems and services used for the Processing of Personal Data and shall regularly review the effectiveness of such measures.
- e) apsware shall take appropriate measures to ensure that Personal Data relating to the Customer is protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.
- f) apsware has appointed a Data Protection Officer. The contact details of the Data Protection Officer are provided in Annex IV for information purposes. apsware may update these contact details from time to time without requiring an amendment to this DPA. apsware shall ensure that the current contact details remain available to the Customer.

7.5 Sensitive data

- a) Where the Processing includes special categories of Personal Data within the meaning of Article 9 GDPR or Personal Data relating to criminal convictions and offences within the meaning of Article 10 GDPR, apsware shall apply appropriate additional safeguards taking into account the nature of such Personal Data and the risks associated with the Processing.
- b) Such Personal Data shall be Processed only where required for the provision of the services under the Main Contract or pursuant to documented instructions from the Customer.

7.6 Documentation and compliance

- a) apsware shall make available to the Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and this DPA.
- b) Upon reasonable request, apsware shall provide the Customer with information regarding its technical and organisational measures and other documentation reasonably necessary to demonstrate compliance.
- c) The Customer may conduct an audit itself or appoint an independent auditor where reasonably necessary to verify apsware's compliance with this DPA. Unless there are reasonable indications of a Personal Data Breach or material non-compliance, audits shall be conducted upon reasonable prior notice, during normal business hours and in a manner that avoids unnecessary disruption to apsware's business operations.
- d) Any auditor appointed by the Customer shall be subject to appropriate confidentiality obligations and shall not be a competitor of apsware.
- e) The Customer shall, where appropriate, take into account relevant certifications, audit reports or other compliance documentation made available by apsware before requesting an on-site audit.
- f) apsware shall cooperate with competent supervisory authorities in accordance with applicable Data Protection Laws.

7.7 Use of sub-processors

- a) The Customer grants apsware general authorisation to engage Sub-processors for the Processing of Personal Data in connection with the services under the Main Contract.
- b) The Sub-processors engaged by apsware are identified in Annex III or in a current Sub-processor list otherwise made available by apsware to the Customer.

- c) apsware shall inform the Customer in advance of any intended addition or replacement of a Sub-processor, thereby giving the Customer the opportunity to object to such change on reasonable grounds relating to data protection.
- d) Where the Customer objects on reasonable data protection grounds, the Parties shall cooperate in good faith to find a commercially reasonable solution.
- e) apsware shall enter into a written agreement with each Sub-processor imposing data protection obligations that provide, in substance, an equivalent level of protection for Personal Data as required from apsware under this DPA, to the extent applicable to the services performed by that Sub-processor.
- f) apsware shall remain responsible to the Customer for the performance of its Sub-processors' data protection obligations to the extent required by applicable Data Protection Laws.
- g) Upon reasonable request, apsware shall provide information regarding the data protection obligations imposed on a Sub-processor. apsware may redact information where necessary to protect confidential information, trade secrets or Personal Data.

7.8 International data transfers

- a) apsware shall not transfer Personal Data to a country outside the European Economic Area ("EEA") or to an international organisation unless the requirements of Chapter V GDPR are complied with.
- b) Where a transfer of Personal Data requires an appropriate safeguard under Article 46 GDPR, apsware shall ensure that an appropriate transfer mechanism is in place, including, where applicable, the Standard Contractual Clauses adopted by the European Commission.
- c) Where apsware engages a Sub-processor that Processes Personal Data outside the EEA, apsware shall ensure that the requirements of Chapter V GDPR applicable to such transfer are satisfied.
- d) apsware shall, upon reasonable request, provide the Customer with information regarding the applicable transfer mechanism.

Clause 8 (Assistance to the Customer)

- a) Taking into account the nature of the Processing, apsware shall assist the Customer by appropriate technical and organisational measures, insofar as reasonably possible, in fulfilling the Customer's obligations to respond to requests from Data Subjects exercising their rights under Chapter III GDPR.
- b) If apsware receives a request from a Data Subject relating to Personal Data Processed on behalf of the Customer, apsware shall inform the Customer without undue delay and shall not respond to the request itself unless authorised to do so by the Customer or required by applicable law.
- c) Taking into account the nature of the Processing and the information available to apsware, apsware shall reasonably assist the Customer in complying with its obligations under Articles 32 to 36 GDPR, including, where applicable:
 - (1) ensuring the security of Processing;
 - (2) assessing and notifying Personal Data Breaches;
 - (3) carrying out data protection impact assessments; and
 - (4) consulting competent supervisory authorities where required.

- d) apsware shall inform the Customer without undue delay if it becomes aware that Personal Data Processed on behalf of the Customer is inaccurate or outdated, insofar as this is relevant to the services provided under the Main Contract.
- e) The scope and manner of apsware's assistance shall take into account the nature and scope of the services under the Main Contract and the information available to apsware.

Clause 9 (Personal Data Breaches)

- a) apsware shall notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Personal Data Processed by apsware on behalf of the Customer.
- b) To the extent the relevant information is available to apsware, the notification shall include:
 - (1) a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
 - (2) the likely consequences of the Personal Data Breach;
 - (3) the measures taken or proposed to be taken by apsware to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; and
 - (4) contact details of a contact point from which further information may be obtained.
- c) Where it is not possible to provide all information at the same time, apsware may provide the information in phases without undue further delay as additional information becomes available.
- d) Taking into account the nature of the Processing and the information available to apsware, apsware shall reasonably cooperate with and assist the Customer in fulfilling the Customer's notification and communication obligations under Articles 33 and 34 GDPR.
- e) apsware shall take appropriate and reasonable measures to investigate, contain and mitigate the effects of a Personal Data Breach and to prevent a recurrence, where reasonably possible.
- f) apsware shall not notify a supervisory authority or affected Data Subjects on behalf of the Customer unless instructed to do so by the Customer or required by applicable law.

SECTION III – FINAL PROVISIONS

Clause 10 (Termination, Return and Deletion of Personal Data)

- a) If apsware is in material breach of this DPA or applicable Data Protection Laws, the Customer may instruct apsware to suspend the affected Processing until apsware has remedied the breach or the Main Contract is terminated in accordance with its terms.
- b) apsware shall inform the Customer without undue delay if apsware is unable to comply with its obligations under this DPA.
- c) Where apsware has informed the Customer in accordance with Clause 7.1 that an instruction infringes applicable Data Protection Laws and the Customer nevertheless insists on that instruction, apsware may suspend the affected Processing and, where continued performance is not reasonably possible, terminate the affected services in accordance with the Main Contract.

- d) Upon termination or expiry of the Main Contract, and subject to the Customer's documented instructions, apsware shall delete or return to the Customer all Personal Data Processed on behalf of the Customer and delete existing copies, unless Union or Member State law requires continued retention of such Personal Data.
- e) Where applicable law requires apsware to retain Personal Data after termination or expiry of the Main Contract, apsware shall continue to protect such Personal Data in accordance with this DPA and shall not Process it for any other purpose than compliance with the applicable retention obligation.
- f) Upon reasonable request, apsware shall confirm the deletion of Personal Data in accordance with this Clause.

Clause 11 (Liability and Costs)

- a) The Parties' liability in connection with the Processing of Personal Data shall be governed by Article 82 GDPR and any other mandatory provisions of applicable Data Protection Laws.
- b) To the extent permitted by applicable law, the liability provisions agreed in the Main Contract shall also apply to this DPA.
- c) Unless otherwise agreed in the Main Contract, no separate remuneration shall be payable to apsware solely for the Processing of Personal Data in accordance with this DPA.

Clause 12 (Miscellaneous)

- a) Any amendments or supplements to this DPA shall be made in documented form, unless a stricter form is required by applicable law.
- b) If any provision of this DPA is or becomes invalid or unenforceable, the remaining provisions shall remain unaffected.
- c) The governing law and jurisdiction agreed in the Main Contract shall also apply to this DPA, unless mandatory provisions of applicable Data Protection Laws require otherwise.
- d) If Personal Data or data carriers belonging to or relating to the Customer are affected by insolvency proceedings, seizure, attachment or similar measures by third parties, apsware shall inform the Customer without undue delay to the extent legally permitted.
- e) apsware shall not assert any right of retention over Personal Data Processed on behalf of the Customer where such retention would prevent the return or deletion of Personal Data required under this DPA, except to the extent such retention is required or permitted by mandatory law.

Annexes

Annex I – Description of Processing

Annex II – Technical and Organisational Measures

Annex III – List of Sub-processors

Annex IV – Data protection contact information

ANNEX I

DESCRIPTION OF PROCESSING

Categories of Data Subjects

Depending on the services provided under the Main Contract, the Personal Data Processed by apsware may relate in particular to the following categories of Data Subjects:

- employees, contractors and other personnel of the Customer;
- customers, prospective customers and business partners of the Customer;
- suppliers, service providers and consultants of the Customer;
- authorised representatives and contact persons of the Customer or its business partners;
- users of systems, applications or services made available, supported or maintained by apsware on behalf of the Customer; and
- other individuals whose Personal Data is provided to or made accessible to apsware by or on behalf of the Customer in connection with the services under the Main Contract.

The categories of Data Subjects actually concerned depend on the services ordered by the Customer and the Personal Data made available to apsware under the Main Contract.

Categories of Personal Data

Depending on the services provided under the Main Contract, the Personal Data Processed by apsware may include in particular:

- identification and contact data, such as names, business contact details and identification or reference numbers;
- professional and organisational data, such as employer, job title, department, function and responsibilities;
- account, user and access data, such as usernames, user IDs, access rights and authentication-related information;
- technical and usage data, such as IP addresses, online identifiers, system and application information, log data and access records;
- customer, supplier, service provider and business partner data;
- contract and business relationship data, including contract master data and information relating to the relevant products or services;
- communication data and information contained in correspondence, support requests or other communications;
- billing and payment-related data, where relevant to the services; and
- other Personal Data contained in systems, applications, files or other data sets made available to or accessible by apsware on behalf of the Customer in connection with the services under the Main Contract.

The specific categories and scope of Personal Data Processed depend on the services ordered by the Customer and the Personal Data provided to or made accessible to apsware by or on behalf of the Customer.

Special Categories of Personal Data

apsware does not intend to Process special categories of Personal Data within the meaning of Article 9 GDPR as a regular element of the services.

Depending on the services provided under the Main Contract and the Personal Data made available to or accessible by apsware on behalf of the Customer, such Personal Data may nevertheless be contained in Customer systems, applications, files or other data sets.

To the extent that apsware Processes special categories of Personal Data within the meaning of Article 9 GDPR, or Personal Data relating to criminal convictions and offences within the meaning of Article 10 GDPR, such Processing shall be limited to what is necessary for the provision of the services and shall be carried out only in accordance with the Customer's documented instructions and applicable Data Protection Laws.

Additional Safeguards

Where special categories of Personal Data or Personal Data relating to criminal convictions and offences are Processed, apsware shall apply appropriate additional safeguards, which may include, as applicable:

- strict purpose limitation;
- access restrictions based on the need-to-know principle;
- confidentiality obligations for authorised personnel;
- appropriate logging and monitoring of access;
- appropriate encryption and other technical security measures;
- restrictions on onward transfers; and
- the technical and organisational measures set out in Annex II.

Nature and Types of Processing

Depending on the services provided under the Main Contract, the Processing operations performed by apsware on behalf of the Customer may include, as applicable:

- collection, recording, organisation and structuring of Personal Data;
- storage, hosting and retention of Personal Data;
- consultation, retrieval, access and use of Personal Data;
- adaptation, alteration, matching or comparison of Personal Data;
- transmission or other provision of Personal Data where required for the performance of the services;
- restriction, deletion or destruction of Personal Data; and
- other Processing operations reasonably necessary to provide the services under the Main Contract in accordance with the Customer's documented instructions.

The specific nature and extent of the Processing depend on the services ordered by the Customer under the Main Contract.

Subject Matter and Purpose of the Processing

The subject matter of the Processing is the Processing of Personal Data by apsware on behalf of the Customer to the extent necessary to provide the services agreed in the Main Contract.

The purpose of the Processing is the performance of the services under the Main Contract in accordance with the Customer's documented instructions. Depending on the services ordered, this may include, in particular, the provision, operation, support, maintenance, administration or other technical servicing of software, systems or applications used by or on behalf of the Customer.

apsware shall not Process Personal Data for purposes other than those necessary to perform the services under the Main Contract or as otherwise instructed by the Customer in accordance with this DPA, unless required by applicable law.

Duration of processing

The Processing shall continue for the duration of the Main Contract and for as long as apsware Processes Personal Data on behalf of the Customer in connection with the services.

Following termination or expiry of the Main Contract, apsware may continue to Process Personal Data only to the extent necessary to return or delete such Personal Data in accordance with this DPA or where retention is required by applicable law.

Further details regarding the duration and termination of the Processing are set out in Clause 4 and Clause 10 of this DPA.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

INCLUDING MEASURES TO ENSURE DATA SECURITY

apsware implements and maintains appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing.

The measures described below are intended to ensure, as appropriate, the confidentiality, integrity, availability and resilience of systems and services used for the Processing of Personal Data.

apsware regularly reviews and, where necessary, updates these measures. Individual measures may be replaced by equivalent or more effective measures, provided that the overall level of security is not materially reduced.

1. Confidentiality pursuant to Article 32 (1) GDPR

1.1 Physical access control

Technical measures	Organisational measures
[x] Alarm system	[x] Key policy / list
[x] Automatic access control system	[x] Visitor log / visitor protocol
[x] Chip cards / transponder systems	[x] Visitors accompanied by employees
[x] Manual locking system	[x] Careful selection of security personnel
[x] Security locks	[x] Careful selection of cleaning services
[x] Locking system with code lock	
[x] Doors with external knob	
[x] Doorbell system with camera	
[x] Video surveillance of entrances	

Secure access to operational buildings and rooms and the authorisation of entitled persons is ensured by apsware, e.g. through:

- Personal checks
- Use of door locking systems and technical monitoring systems
- Issuing additional security keys in individual cases

1.2 Logical access control

Technical measures	Organisational measures
[x] Login with username + password	[x] Management of authorisations
[x] Anti-virus software server	[x] Creation of user profiles
[x] Anti-virus software clients	[x] Central password allocation
[x] Firewall	[x] "Secure password" policy
[x] Intrusion detection systems	[x] "Deletion / destruction" policy

☒ Use of VPN for remote access	☒ "Clean desk" policy
☒ Encryption of data carriers	☒ General data protection and/or security policy
☒ Encryption of smartphones	☒ Mobile device policy
☒ BIOS protection (separate password)	☒ Guidance "Manual desktop lock"
☒ Automatic desktop lock	
☒ Encryption of laptops/tablets	

Further measures:

Access authorisation is granted on the basis of an application procedure involving the information owners. Ideally, further control instances are integrated into the approval process. Technical authorisation is usually implemented via recognised security systems such as ActiveDirectory (Windows), LDAP (Linux) or RACF (Mainframe).

Execution of access is technically monitored, logged and controlled.

1.3 Data access control

Technical measures	Organisational measures
☒ Paper shredder (at least level 3, cross cut)	☒ Use of authorisation concepts
☒ External document destruction service (DIN 32757)	☒ Minimum number of administrators
☒ Physical deletion of data carriers	☒ Administration of user rights by administrators
☒ Logging of access to applications, specifically when entering, modifying and deleting data	

2. Integrity (Article 32(1)(b) GDPR)

2.1 Transfer control

Technical measures	Organisational measures
☒ Email encryption	☒ Documentation of data recipients and planned transfer duration / retention or deletion periods
☒ Use of VPN	☒ Overview of regular retrieval and transmission processes
☒ Logging of access and retrieval	☒ Transfer in anonymised or pseudonymised form
☐ Secure transport containers	☐ Due care in selecting transport staff and vehicles
☒ Provision via encrypted connections such as sftp, https	☐ Personal handover with protocol
☐ Use of signature procedures	

2.2 Input control

Technical measures	Organisational measures
[x] Technical logging of the entry, modification and deletion of data	[x] Overview of which programs can be used to enter, modify or delete which data
	[x] Traceability of entry, modification and deletion by individual usernames (not user groups)
	[x] Allocation of rights to enter, modify and delete data based on an authorisation concept
	[x] Clear responsibilities for deletions

3 Availability and resilience (Article 32(1)(b) GDPR)

3.1 Availability control

Technical measures	Organisational measures
[x] Fire and smoke detection systems	[x] Backup & recovery concept (detailed)
[x] Fire extinguisher in server room	[x] Monitoring of backup processes
[x] Server room monitoring (temperature and humidity)	[x] Regular tests of data recovery and logging of results
[x] Air-conditioned server room	[x] Storage of backup media in a secure place outside the server room
[x] UPS	[x] Separate partitions for operating systems and data
[x] Protected power strips (server room)	
[x] RAID system / disk mirroring	
[x] Video surveillance server room	
[x] Alarm notification in case of unauthorised access to the server room	

4. Regular review, assessment and evaluation (Article 32(1)(d) GDPR; Article 25(1) GDPR)

4.1 Data protection management

Technical measures	Organisational measures
[] Software solutions for data protection management in use	[x] Internal/external Data Protection Officer (name/company/contact details)
[x] Central documentation of all procedures and rules on data protection with access for employees via the DPO	[x] Employees trained and bound to confidentiality/data secrecy

☐ Security certification according to ISO 27001, BSI IT-Grundschutz or ISIS12	☒ Regular awareness-raising of employees at least annually
☒ Other documented security concept	☒ Internal/external information security officer (name/company/contact)
☒ Review of effectiveness of technical safeguards at least annually	☒ Data protection impact assessment (DPIA) carried out where required
	☒ Organisation complies with information obligations under Articles 13 and 14 GDPR
	☒ Formalised process for handling data subject access requests exists

4.2 Incident-Response-Management

Support in responding to security incidents

Technical measures	Organisational measures
☒ Use of firewall and regular updates	☒ Documented process for detecting and reporting security incidents/data breaches (including notification duties to supervisory authority)
☒ Use of spam filter and regular updates	☒ Documented procedures for handling security incidents
☒ Use of antivirus scanner and regular updates	☒ Involvement of DPO and information security officer in incidents/breaches
☒ Intrusion Detection System (IDS)	☒ Documentation of incidents/breaches e.g. via ticket system
☒ Intrusion Prevention System (IPS)	☒ Formal process and responsibilities for post-processing of incidents/breaches

4.3 Data protection by default (Article 25(2) GDPR)

Technical measures	Organisational measures
☒ No more personal data are collected than necessary for the respective purpose	☒ Easy exercise of the data subject's right of withdrawal by technical measures

4.4 Processing control (outsourcing to third parties)

Technical measures	Organisational measures

	[x] Prior review of the Sub-processor's security measures and documentation thereof
	[x] Selection of the Sub-processor with due diligence (especially regarding data protection and information security)
	[x] Conclusion of the required data processing agreement and/or EU standard contractual clauses
	[x] Written instructions to the Sub-processor
	[x] Binding of the Sub-processor's employees to confidentiality
	[x] Obligation to appoint a data protection officer where required
	[x] Agreement of effective audit rights vis-à-vis the Sub-processor
	[x] Rules on engaging further Sub-processors
	[x] Ensuring destruction of data after termination
	[x] For long-term cooperation: ongoing review of the Sub-processor and its security level

ANNEX III
LIST OF SUB-PROCESSORS

The Customer grants apsware general authorisation to engage the Sub-processors listed below in accordance with Clause 7.7 of this DPA.

apsware may add or replace Sub-processors in accordance with the procedure set out in Clause 7.7. The current list of Sub-processors applicable to the services under the Main Contract shall be made available to the Customer by apsware.

Sub-processor	Services / Processing activities	Location of Processing	Transfer mechanism, if applicable
Salesforce.com Germany GmbH, Erika-Mann-Strasse 31-37, 80636 München	CRM system services	Europe	
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur	Webpage and email services	Germany	
Proton AG, Route de la Galaise 32, 1228 Plan-les-Ouates, Geneva, Switzerland	Email services	Switzerland	



ANNEX IV

DATA PROTECTION CONTACT INFORMATION

General Data Protection Contact

Company: apsware GmbH
Address: Am Hockeypark 10, 41179 Mönchengladbach, Germany
Email: datenschutz@apsware.com

Data Protection Officer

Name: Daniela Heinke
Telephone: +49 2161 823 7799
Mobile: +49 170 440 4539
Email: datenschutz@apsware.com

Updates to Contact Information

The contact details provided in this Annex are supplied for information and communication purposes. apsware may update these details from time to time without requiring an amendment to the DPA. apsware shall ensure that current contact information remains available to the Customer.

Version / Last updated: October 8th, 2026