Commissioned Data Processing Agreement

in accordance with Article 28 of the GDPR

between the

– Controller – hereinafter referred to as Client -

and

PROSTEP AG
Dolivostraße 11
64293 Darmstadt

– Processor – hereinafter referred to as Contractor -

PREAMBLE

The following data protection and data security provisions apply to all contractual services involving the commissioned processing of data provided to the Client by the Contractor and to all activities in which the Contractor's employees or third parties commissioned by the Contractor may come into contact with personal data from the Client (contractual agreements in this context are hereinafter referred to as the main contract).

1 DESCRIPTION OF SERVICES

1.1 Within the framework of the contract, the Contractor processes personal data on behalf of the Client for the purpose of providing the Client with the services described in **Annex 1 (Description of Services)**. The subject matter, the duration of the contract, the nature and purpose of the processing, the type of personal data and the categories of data subjects are described in the annex.

1.2 The Client may terminate the contract at any time without notice if there is a serious violation by the Contractor of the provisions stipulated in this contract, if the Contractor is unable or unwilling to carry out an instruction issued by the Client or if, in violation of the contract, the Contractor refuses to carry out contractual or statutory inspection measures stipulated by the Client.

2 TECHNICAL AND ORGANIZATIONAL MEASURES

2.1 Prior to the commencement of processing, the Contractor must document the execution of the requisite technical and organizational measures specified in advance of awarding the contract, in particular those relating to execution of the contract, and present the documentation to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as an inspection/audit by the Client indicates a need for adaptations, such adaptations must be implemented by mutual agreement.

2.2 The Contractor must ensure security in accordance with Art. 28 para. 3(c) and Art. 32 GDPR, in particular in conjunction with Art. 5 para. 1 and para. 2 GDPR. The measures to be taken comprise data security measures and measures that guarantee a level of protection appropriate to the risk in terms of confidentiality, integrity, availability and resilience of the systems. The state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing (resulting from possible loss, alteration, destruction, unauthorized access or disclosure) within the meaning of Art. 32 para. 1 GDPR must be taken into account.

2.3 The technical and organizational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement adequate alternative measures. In so doing, the security level of the defined measures must not be reduced in any way.

2.4 Substantial changes must be documented and communicated to the Client without delay (in at least text form). If substantial changes are made to the technical and organizational measures, these must be coordinated with the Client. The changes must be agreed in writing and become part of the contract in accordance with **Annex 2 (Technical and Organizational Measures)**. Coordination is not, however, required if the changes result in an improvement of the level of data protection agreed within the

framework of this agreement on commissioned data processing and the Client is informed of these changes. Once the Client is provided with the corresponding information, the changes automatically become part of the contract; **Annex 2 (Technical and Organizational Measures)** must be modified accordingly.

2.5 The processing of personal data in a private residence or within the framework of telecommuting must be coordinated with the Client and documented. The Client has the right to object. If the Client does not exercise this right within 14 days of the information concerning the processing referred to in this paragraph being made available, this will be deemed as approval. If services or work is performed in a private residence or in the form of telecommuting, the Contractor must ensure compliance with special data protection measures as are necessary within the context of Art. 32 GDPR.

3 RECTIFICATION, BLOCKING AND ERASURE OF DATA

3.1 The Contractor may only rectify, erase, block or restrict the processing of data that is being processed on behalf of the Client upon instruction by the Client. If a data subject contacts the Contractor directly in this regard, the Contractor must immediately forward the data subject's request to the Client.

3.2 Unless the parties have agreed otherwise in the main contract, erasure policy, the "right to be forgotten", rectification, data portability and information must be ensured by the Contractor in accordance with the documented instructions of the Client without delay.

4 CONTROLS AND OTHER DUTIES OF THE CONTRACTOR

4.1 The Contractor undertakes to process personal data only upon documented instruction by the Client.

4.2 The Contractor must ensure that all persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have been familiarized with the relevant data protection provisions before any work is performed. Section 4.1 applies to these persons accordingly.

4.3 Taking the nature of the processing and the information available to the Contractor into account, the Contractor must assist the Client to the best of its ability in complying with the Client's obligations regarding the security of the processing, reporting violations of the protection of personal data to supervisory authorities and the respective data subjects, with data protection impact assessments and with any resulting need for consultation with supervisory authorities.

4.4 The Contractor must submit to any inspection measures stipulated by the data protection authorities and must inform the Client immediately in text form of inspection measures insofar as they relate to the contract with the Client. This also applies if a competent authority is conducting an investigation in connection with non-compliance procedures or criminal proceedings involving the commissioned processing of personal data by the Contractor. If the Client is subject to an inspection by the supervisory authority, non-compliance procedures or criminal proceedings, a liability claim made by a data subject or by a third party, or any other claim in connection with the commissioned processing of data by the Contractor, the Contractor must make every

effort to support the Client. These support services include providing information and are only to be carried out if they are legally possible and the time and effort involved is reasonable. In particular, the Contractor has no obligation to bear any costs.

4.5 The Contractor is obliged to observe the relevant regulations regarding the appointment of a data protection officer. The Client must be informed of the data protection officer's contact details for the purpose of direct contact. The current data protection officer is (name, address, contact data):

Mr. Nadi Sönmez, PROSTEP AG, Dolivostr. 11, 64293 Darmstadt
E-mail: datenschutz@prostep.com, Tel: 06151 9287 316

The Client must be informed immediately in text form of any change of data protection officer.

4.6 The Contractor is obliged to periodically monitor the technical and organizational measures and the internal processes. The Contractor must ensure the verifiability of the technical and organizational measures taken vis-à-vis the Client.

4.7 The Contractor must keep a list of all the categories of processing activities carried out on behalf of the Client.

4.8 The Contractor must immediately inform the Client in text form if they are of the opinion that an instruction violates German or European data protection regulations.

4.9 Taking into account the nature of the processing, the Contractor must assist the Client in accordance with Art. 28 para. 3 sentence 2 point e) GDPR by taking appropriate technical and organizational measures, insofar as this is possible, to ensure that the Client can meet its obligation to respond to requests for exercising the data subject's rights specified in Art. 12 to 23 GDPR.

5 SUBCONTRACTING

5.1 Subcontracting for the purpose of this regulation is understood to mean services that 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 or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. The Contractor is, however, 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 Client's data, even in the case of outsourced ancillary services.

5.2 The Contractor may only commission subcontractors (additional processors) with prior explicit written or documented consent from the Client.

5.3 If a subcontractor is used, the Contractor must conclude a contract with the subcontractor in accordance with Art. 28 GDPR relating to the processing of data on behalf of the Client. The subcontract must be in writing. The contract must impose on the subcontractor the same obligations regarding the protection of personal data as specified in the contract between the Client and the Contractor.

5.4 If a subcontractor fails to comply with its data protection obligations, the Contractor is liable to the Client for ensuring compliance with the obligations by every subcontractor. The general provisions governing the relationship between the Contractor and the subcontractor remain unaffected.

5.5 **Annex 3 (Subcontracting Relationships)** to this contract lists all the Contractor's subcontractors at the time the contract was concluded.

5.6 The transfer of personal data from the Client to the subcontractor is only permitted when all requirements for a subcontract have been met.

5.7 The service contractually agreed in Annex 1 is provided exclusively in Germany and thus in a Member State of the EU or in a Member State of the European Economic Area (EEA). Any transfer of the service to be rendered, or of any part of the work to be performed, to a third country requires the prior agreement of the Client in text form and may take place if the special requirements of Art. 44 ff DSGVO are fulfilled (e.g. adequacy decision by the Commission, standard protection clauses, approved rules of conduct).

5.8 Further outsourcing by the subcontractor requires the express consent of the Client in text form.

6 SUPERVISORY POWERS OF THE CLIENT

6.1 The Contractor grants the Client and/or its authorized representative the right to carry out inspections of the data protection and data security precautions taken.

6.2 This right of inspection is intended to verify compliance with the Contractor's obligations in its business operations. In addition to on-site inspections, evidence of compliance can also be provided by means of independent test reports and certifications. If on-the-spot checks are to be performed, they must be designed as random checks and must ordinarily be announced in good time. The interval at which inspections are performed is based on necessity. The Contractor must also provide the Client with all the necessary information. Exercising the right to carry out inspections must not unduly disrupt business operations nor may it be abusive in nature.

6.3 The Client will not reimburse any costs for inspections relating to data protection carried out at the Contractor's premises.

7 COMMUNICATION IN THE CASE OF VIOLATIONS BY THE CONTRACTOR

7.1 The Contractor is obliged to inform the Client in text form without delay, but within no more than 24 hours, if there is a reasonable suspicion of a violation of the data protection and data security provisions laid down in this contract by the Contractor or by third parties the Contractor has commissioned. The same applies to violations of the general rules on the protection of personal data.

7.2 The Contractor must provide the Client with sufficient information to enable the Client to comply with its obligation to notify the relevant authority and to inform the data subject concerned without delay, but no later than 36 hours after a personal data breach

becomes known. The Contractor is not authorized to inform the data subject concerned about the personal data breach. The Contractor must cooperate with the Client and take reasonable steps to assist the Client with investigating, mitigating and rectifying any such personal data breach, with data protection impact assessments, and with regard to prior consultation with the supervisory authority.

8 AUTHORITY OF THE CLIENT TO ISSUE INSTRUCTIONS

8.1 The Contractor and any person subordinate to the Contractor who has access to personal data may process such data only within the framework of the Client's instructions, including the powers granted in this contract, unless they are legally required to process the data.

8.2 If the Contractor is unable to comply with an instruction, the Contractor is obliged to inform the Client immediately in text form. In this case, the Client is entitled to suspend the transfer of data and/or to withdraw from this contract and from the main contract for which this contract was concluded.

8.3 The Client must confirm oral instructions in text form without delay.

8.4 The Contractor must immediately notify the Client in text form of any instruction given by the Client which, in the Contractor's opinion, violates data protection regulations. The Contractor is entitled to suspend execution of the corresponding instruction until it has been confirmed or amended by the Client in text form.

9 ERASURE AND RETURN OF PERSONAL DATA

9.1 Copies and duplicates of the data must not be made without the knowledge of the Client, with the exception of backup copies insofar as they are needed to ensure proper data processing and data required to meet statutory retention obligations.

9.2 After conclusion of the contracted work, or earlier upon request by the Client or upon completion or termination of this contract, the Contractor must hand over to the Client all documents, processing and utilization results, and data sets related to the contract that have come into the Contractor’s possession or, subject to prior consent by the Client in text form, destroy them in accordance with data protection regulations. The erasure and destruction of all the data in its entirety must be performed using recognized, state-of-the-art procedures for overwriting data multiple times. The same also applies to test, waste, redundant and discarded material, which is to be kept under lock and key in compliance with data protection regulations until it is erased or returned. The log of the deletion must be presented to the Client upon request and a copy handed over.

9.2 Data must not be deleted or destroyed as far as and for as long as the Contractor requires the data for its own legitimate purposes, in particular to provide documented proof of orderly data processing (e.g. when invoicing the Client), or as far as and for as long as the Contractor is obliged to store the data due to statutory regulations or official directives.

10 OTHER REGULATIONS

10.1 The Contractor must inform the Client immediately if fulfillment of this contract in accordance with section 1 of this agreement is jeopardized by the Contractor due to seizure or confiscation, insolvency or composition proceedings or other events or measures taken by third parties. The Contractor must immediately inform all the parties involved in this context that the Client has sole power of disposition of the data.

10.2 In the event of any conflicts between this contract and a main contract, the provisions in this contract take precedence over the provisions in the main contract.

10.3 Should any provision in this contract be found invalid, this will not affect the validity of the rest of the contract.

10.4 Any amendment to this agreement, including its termination, and this clause must be in written form, including in an electronic format.

SIGNATURES

For the Client:

Darmstadt, (date)

_____

(signature)

_____

(print name)

_____

(role/position)

For the Contractor:

Darmstadt, (date)

_____

(Signature)

Dr. Bernd Pätzold

(print name)

Chief Executive Officer

(role / position)

Annex 1 - DESCRIPTION OF SERVICES

1. SUBJECT MATTER AND DURATION OF THE CONTRACT

(1) SUBJECT MATTER

☒ The subject matter of the contract involving the handling data is the execution of the following tasks by the Contractor:
The subject matter of the contract is the service defined in the letter of tender for the scope of service as regards GlobalX SaaS. With regard to the GDPR, it should be pointed out that the setting up and maintenance of users and data exchange partners (processing of personal data) is performed by the Client. PROSTEP is responsible for operating the systems and providing 2nd level support if required. PROSTEP's product support staff have access to the applications and can view and, if necessary, process personal data.

(2) DURATION

☒ The duration of this contract (term) corresponds to the term of the service agreement.

2. CONTRACT CONTENT IN GREATER DETAIL

(1) TYPE AND PURPOSE OF THE PLANNED DATA PROCESSING

☒ More detailed description of the subject matter of the contract with regard to the nature and purpose of the tasks performed by the Contractor:
In the context of IT system administration and 2nd level support, it may be necessary to access data from OpenDXM GlobalX and the associated Oracle database, from which personal data belonging to the users and data exchange partners set up in the system can be seen. This is personal data in the form of user data that is collected when the data exchange processes are used, such as first name, last name, department/group, company affiliation, telephone numbers (business), e-mail address (business), ENGDAT routing addresses if applicable, role assignment, place of work, usage behavior, time stamps in log files, assignment of the user data sent and received , etc., and is not used for any other purpose.

(2) TYPE OF DATA

☐ The following data types/categories are subject of the processing of personal data (list/description of the data categories):

- ☒ Personal master data
- ☒ Communication data (e.g. telephone, e-mail)
- ☒ Contract master data (contractual relationship, product/contractual interest)
- ☒ Customer history
- ☒ Data transfer history (e.g. database, log files)
- ☒ Hotline and support inquiries
- ☒ Contract billing and payment data
- ☐ Planning and control data
- ☐ Information (from third parties, e.g. credit agencies, public directories)
- ☐ Click here to enter text

(3) CATEGORIES OF DATA SUBJECTS

☐ The categories of persons affected by processing include:

- ☒ Customers
- ☒ Client's data exchange partners
- ☐ Interested parties
- ☒ Employees
- ☐ Suppliers
- ☐ Sales representatives
- ☒ Contact persons
- ☐ Click here to enter text

ANNEX 2 - TECHNICAL AND ORGANIZATIONAL MEASURES

Taking into account the

- state of the art,

- cost of implementation and
- the nature, scope, context and
- purposes of processing as well as
- the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing,

the Contractor must take appropriate technical and organizational measures to ensure a level of protection commensurate with the risk.

The Contractor must take the following measures:

1. Physical access control measures

Measures	**Description**
Specification of authorized persons (company employees and external persons)	The definition of what constitutes an authorized person is clearly regulated. Physical access is authorization-specific. The company building can only be accessed using a (personal) transponder. Within the building, access to areas with increased security needs (IT administration) is secured using additional authorization levels. Access authorizations are granted exclusively on the basis of employees' areas of activity.
Rules for visitors	Visitors must register at the reception desk. They are picked up at the reception desk. Visitors are always be accompanied by an employee while on the company premises. Once a visit has ended, the visitor is accompanied to the exit.
Recording/identifying visitors	All visitors are registered at the reception desk. Visitors are given a visitor pass that must be worn where it can be seen.
Rules regarding keys	All transponders and keys are documented in a key list that is updated daily.

2. Electronic access control measures

Measures	**Description**

Request to set up user accounts	Authorization to set up or modify user accounts is granted once a review and approval process has been completed.
Data processing systems are protected by login procedures	Access is password-protected, and the access data is only made known to selected employees.
Password policy (length, interval at which passwords must be changed, etc.)	at least 11 characters upper/lowercase, numbers, special characters 3 of the 4 criteria must be met Min. password age: 1 day Max. password age: 180 days Password security policies and defaults exist and are checked automatically.
Security measures when leaving the workplace	Users lock their PCs when leaving their workspace. PCs are also locked after 10 minutes of inactivity.
Passwords are locked after multiple failed attempts	Failed logins are logged. Employee PCs are automatically locked if the wrong password is entered 3 times.
Regulations/requirements for telecommuting	Within the context of the contractual relationship, telecommuting workstations may only be set up with the Client's consent.
Protection of the network connection for telecommuting (e.g. VPN, access token)	If telecommuting workstations are set up with the consent of the Client, access is protected using a VPN connection with OTP.
One user master record per user is set up (no group accounts)	All persons/employees have their own separate user account.
Data and document storage	Digital data is stored on secure systems. Non-digital data/documents are stored in locked cabinets/containers. Data carriers that are no longer being used in the production process are disposed of by certified disposal companies in accordance with data protection regulations. The use of USB memory devices is only permitted in encrypted form and on PROSTEP's own hardware. The loss of mobile devices (e.g. if a company car is broken into) must be reported immediately. These devices are immediately blocked for access to internal networks.

3. Internal access control measures

Measures	Description
Central user rights registry	Central systems are used to assign rights to both customers and employees.
Formal application and approval procedure	The scope of an employee's authorization depends on their job/task description. Employees cannot set up rights themselves. Department managers must obtain approval for granting additional rights from IT administration. The HR department must inform IT administration immediately when an employee leaves the company. As soon as an employee leaves, all permissions will canceled and any accesses that have been set up will be deleted.
Access authorizations are regulated on the basis of defined roles; they are not associated with a specific person	Access to different services and systems is regulated by group guidelines. These are managed centrally. The starting point for granting rights is the employee's job description. The required rights are requested from IT administration by the head of department.
Access rights are updated regularly and are adapted to changing circumstances, e.g. when an employee moves to a different department within the organization	The fact that employees' rights must be adapted accordingly if their responsibilities change is regulated at organizational level.
Time limits for access options	Employees have access to the corresponding data only for as long as they need it to perform their respective tasks.
Guidelines for file organization	Requirements relating to the storage of data or information by employees exist. Employees may only use the software approved by company management within the framework of the authorizations granted to them. Data storage within the software used is determined by the database structure and the rights granted. Drive/folder sharing is only set up if requested by the head of a department. Only employees who are authorized to maintain data have write access to data in the intranet. All employees receive instructions/training relating to the software used and the storage options available within their area of responsibility.
Firewalls	All systems and network segments are fully protected by firewall systems.

4. Data transfer control measures

Measures	Description
Encryption during data transfer	Data transfer operations are always encrypted whenever possible.
Disposal of data carriers and information that are no longer needed in accordance with data protection regulations	Data carriers are physically destroyed. Data is deleted once legal or contractual obligations regarding burden of proof/data retention have expired.
Documentation of the download and transmission programs	All the programs used are documented for both employees and customers.
Documentation of the points at which transmission is provided and of the transmission channels used (configuration)	All transmission procedures are documented. Mobile data carriers are not used. Couriers are therefore not used.
Authorized users with special rights	Some authorized users for different work areas are granted special rights with regard to personal data, as these rights are needed to perform day-to-day work or for troubleshooting.
Remote maintenance concept	Type, scope and authorizations for remote maintenance are documented and implemented using management tools. Access to the Client's systems can be web-based. This applies to both the Contractor and the Client. Upon request, access by the Contractor can always be announced/approved by telephone.

5. Data entry control measures

Measures	Description
Proof of the data entry-related responsibilities defined at organizational level	Authorization for the input/processing of data by the relevant persons is regulated.
Process, program and workflow organization	Basic documentation exists for all relevant activities.
Authenticity	If necessary, logs can be viewed to see when which user has created, edited or deleted data. User identification is ensured by means of authentication during login.

6. Contract control measures

Measures	Description
Selection of (sub)contractors	The selection of a (sub)contractor is made after careful examination of their reliability as regards data protection. The Contractor's data protection officer examines the suitability of the data protection measures taken by a subcontractor.
Regular monitoring of the Contractor's compliance with data protection regulations	An inspection by the Client (e.g. on-site inspection by an expert) is possible at any time after prior notification. In this specific case, no inspection is necessary as there are no subcontractors.

7. Availability control measures

Measures	Description
Backup	An up-to-date backup concept exists for the computer center operated by the Contractor. Backup is performed as a disaster recovery backup and every 12 weeks as an archival backup. In addition, all infrastructure VMs are backed up daily. This backup is stored for 3 days. The backup of the VMs is independent of the applications running on the VM. Recovery using this backup is always performed as a complete VM.
Emergency response	An up-to-date emergency plan exists for the computer center operated by the Contractor. The emergency plan includes information from the data protection officer. Within the scope of their responsibility and taking into account the legal requirements, the data protection officer subsequently collects information from Client and, if applicable, from the supervisory authorities with the consent of the Client.
Safeguards at the data center	– Electronic and mechanical access control systems – Video surveillance and smoke detectors within the data center – Fire-fighting equipment – Air conditioning via 2 separate cooling circuits (n+1) – Redundant power supply

	– Uninterruptible and filtered power supply using UPS batteries (online UPS)
Patch management	Patch management for the environment is performed regularly based on the patches and fixes provided by Microsoft. The Contractor reserves the right to install individual patches and larger service packs subject a reasonable delay for the purpose of collecting empirical values regarding system stability where appropriate.
Virus protection	Key components and all employee systems are protected against viruses. A virus protection concept is included in the operating manual and has been implemented.
Firewalls	Key components and all employee systems are protected against outside attacks. A firewall concept is included in the operating manual and has been implemented.

8. Separation control measures

Measures	**Description**
Client separation	If data belonging to the Client is stored on the Contractor's systems, this data is subject to logical separation when processed.
Functional separation	Functions are separated in accordance with section 8 of the Annex to § 9 sentence 1 BDSG (German Federal Data Protection Act). The Contractor's various organizational units (such as development and support) only have access to the data relevant to their tasks.

Annex 3 - SUBCONTRACTING

When processing data on behalf of the Client, the Contractor makes use of services provided by third parties, who process data on the Contractor's behalf ("subcontractors").

Name and address of subcontractors	Subject matter of the subcontracting	Date of the subcontracting contract
DARZ GmbH *Julius-Reiber-Straße 11* *64293 Darmstadt*	*Deployment of the Open DXM GlobalX SaaS infrastructure in the high-security data center*	*17.09.2018*

Please send this signed agreement in duplicate to:

PROSTEP AG
Attn. Sabine Kölsch
Dolivostr. 11
64293 Darmstadt

We will return a countersigned copy to you without delay.