# DATA PROCESSING AGREEMENT (DPA) PURSUANT TO ART. 28 GDPR

## 1. Object and Duration of this DPA

1.1 The object of this DPA (hereafter also referred to as “Agreement”) is derived from the Contract for SaaS Service and Consulting Services between the Customer and BELLIN, to which reference is made in this document (“Contract”).

1.2 This DPA shall apply for the duration of the Contract between the Parties. Notwithstanding the aforementioned provisions concerning the contract duration, the obligation to comply with data secrecy and confidentiality as well as agreed retention periods shall continue to apply notwithstanding the termination of the Contract.

## 2. Scope, Nature and Purpose of this DPA

2.1 The processing of the personal data by BELLIN on behalf of the Customer as part of the Contractual Services is limited in scope and nature to the personal data entered by (or on behalf of) the Customer in its use of the Services and solely for the purpose of providing to the Customer the full benefit of the Services in accordance with the Contract.

2.2 Data shall be processed exclusively within the Federal Republic of Germany, in a Member State of the European Union, in a State party to the agreement on the European Economic Area, in the EFTA member Switzerland or in Canada. A transfer to a third country other than the aforementioned requires prior informed consent given by the Customer and must comply with the specific requirements put forward in Arts. 44 ff. of the EU General Data Protection Regulation (GDPR). For Switzerland and Canada, an adequate level of protection is established through an Adequacy Decision by the Commission pursuant to Art. 45(3) GDPR. In case of an exit of the United Kingdom from the European Union, an agreement based on the EU model clauses will be put in place between BELLIN and respective subcontractors until an Adequacy Decision for the United Kingdom is made by the Commission.

2.3 If a subcontractor is to be commissioned, these requirements shall apply in addition to the provisions set forth in Clause 6 of this DPA.

2.4 The following types / categories of personal data may be processed:

a) Names and business contact details of users (in particular authorized representatives of accounts)

b) Names and account numbers of creditors and debtors (in particular customers and suppliers)

c) Names and account numbers of employees.

## 3. Technical and Organizational Measures (TOM)

3.1 BELLIN shall ensure the implementation of technical and organizational measures agreed prior to commissioning contract data processing and specified in the agreement schedule prior to commencing data processing, in particular with respect to the actual execution of the contract work and shall give the Customer the opportunity to check and audit these measures at the Customer's own expense and with sufficient advance notice. Upon acceptance of the TOM by the Customer, the Customer shall deem these measures to be a prerequisite of any contract work undertaken. Insofar as the check by the Customer results in a need for adaptation, the Customer shall be entitled to order this adjustment.

3.2 Collectively, the measures to be implemented represent non-contract specific measures pertaining to

a) Physical access control
b) System access control
c) Data access control
d) Separate processing control
e) Pseudonymization
f) Transmission control
g) Input control
h) Availability control
i) Control of processors for regular control, valuation and evaluation

To the extent that these measures do not derive from the underlying Contract, they shall be treated separately in the "General Technical and Organizational Security Measures Pursuant to Art. 28 GDPR" schedule (TOM).

3.3 BELLIN is obligated to guarantee security in accordance with Arts. 28(3)(c), 32 GDPR, in particular in conjunction with Art. 5(1), (2) GDPR. The measures to be undertaken generally represent measures pertaining to data security and the guarantee of a level of protection appropriate to the nature and extent of the risk with regard to confidentiality, integrity, availability and resilience of systems. The state of technology, implementation costs and the type, scope and purposes of processing as well as varying degrees of probability of occurrence and the severity of a risk posed to the rights and freedoms of a natural person pursuant to Art. 32(1) GDPR are to be taken into account [refer to the "General Technical and Organizational Security Measures Pursuant to Art. 28 GDPR (TOM)" schedule for details].The technical and organizational measures are subject to technological progress and development. In this respect, BELLIN shall be entitled to implement suitable alternative measures. Such measures must not fall short of the level of security provided by the measures specified in this document. Major changes must be agreed in writing.

## 4. Correcting, Restricting and Deleting Data

BELLIN is prohibited from correcting, deleting or restricting data to be processed on behalf of the Customer in an unauthorized manner and may only do so upon documented instructions by the Customer, unless a continuing storage of that data of the customer is mandated by law. Should a data subject contact BELLIN directly in this context, BELLIN shall forward this request to the Customer without delay. To the extent covered by the scope, BELLIN shall directly implement deletion concept, the right to erasure, correction, data portability and disclosure of information upon documented instructions by the Customer.

## 5. Quality Assurance and Other Obligations of BELLIN

In addition to complying with the provisions stipulated by this DPA, BELLIN shall have the following obligations pursuant to Arts. 28 through 33 GDPR; in this respect BELLIN shall guarantee compliance with the following provisions:

- In case BELLIN is mandated by the GDPR or corresponding data privacy acts of the member state of the EU in which BELLIN is registered, the appointment in writing of a Data Protection Officer whose responsibilities are outlined in Arts. 38 and 39 GDPR. The Data Protection Officer's contact details are provided to the Customer to enable direct communication. The appointed Data Protection Officer's contact details are listed in the schedule (TOM).
- Maintaining data confidentiality pursuant to Arts. 28(3)(b), 29, 32(4) GDPR. BELLIN shall only entrust employees with the execution of contract work who have been obligated to maintain data confidentiality and who have been instructed on the specific data protection obligations of relevance to them. BELLIN or any persons reporting to BELLIN with access to personal data may only process this data in line with Customer instructions, including the powers set forth in this DPA, unless they are legally required to process data.
- Implementation and compliance with any technical and organizational measures required as part of this DPA pursuant to Arts. 28(3)(c), 32 GDPR [refer to the "General Technical and Organizational Security Measures Pursuant to Art. 28 GDPR (TOM)" schedule for details].
- Upon their request, the Customer and BELLIN shall cooperate with any regulatory authority in the course of the execution of contract work.
- Immediate notification to the Customer of any audit activities and measures initiated by a supervisory authority provided these activities and measures pertain to this DPA. This also applies if a competent authority, within the framework of non-compliance procedures or criminal proceedings, pursues an investigation against BELLIN pertaining to the processing of personal data for the execution of contract work.
- Should the Customer for their part become the subject of an audit by a regulatory authority, non-compliance procedures or criminal proceedings, liability claims by a data subject or a third party or any other claims in connection with contract work performed by BELLIN, then BELLIN shall be obligated to support the Customer as best they can.
- BELLIN shall regularly audit internal processes and technical and organizational measures to ensure compliance with applicable data protection legislation and to guarantee the protection of the rights of data subjects within the scope of their contractual data processing work.
- Providing the Customer with evidence of technical and organizational measures undertaken within the framework of audit rights pursuant to Clause 7 of this DPA
- Reasonable time and material cost for such support services by BELLIN shall be reimbursed by the customer.

## 6. Subcontractual Relationships

6.1 For the purpose of this DPA, subcontractual relationships are defined as any services that arise directly from the principal DPA performance. Not covered are any ancillary services BELLIN makes use of such as telecommunications services, postal/delivery services, maintenance and user services or the disposal of data storage devices or any other measures aimed at ensuring confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. BELLIN is however obligated to enter into suitable and lawful contractual agreements and to implement control measures in connection with ancillary services in the interest of upholding data protection and data security in connection with Customer data.

6.2 The Customer agrees to the commissioning of the following subcontractors subject to a contractual agreement in accordance with Art. 28(2-4) GDPR:

| Subcontractor | Address/country | Service |
|---|---|---|
| BELLIN GmbH | Tullastraße 19<br>77955 Ettenheim<br>Germany | ■ BELLIN Cloud services (excl. “Treasury Connected”)<br>■ Consulting<br>■ Implementation<br>■ Application support |
| BELLIN Treasury Services Ltd. | Suite 1022<br>470 Granville Street<br>Vancouver, BC<br>V6C 1V5<br>Canada | ■ Consulting<br>■ Implementation |
| BELLIN Treasury International GmbH | Tullastr. 19<br>77955 Ettenheim<br>Germany | ■ Customer relationship management<br>■ Customer data maintenance<br>■ Customer services (events, travel arrangements, marketing activities)<br>■ BELLIN Cloud services for “Treasury Connected” |

6.3 Outsourcing for processing personal data of the customer to a subcontractor or a change of subcontractor shall be permitted independent from section 6.2 provided that all of the following conditions are complied with:

a) BELLIN submits such an outsourcing to a subcontractor to the Customer in writing or at least in text form with appropriate advance notice.

b) The Customer has not objected to the planned outsourcing within 14 days of receiving the notice due to good cause which shall be proven to BELLIN (the right for the Customer to object the respective outsourcing shall expire, if the Customer does not object within 14 days of receiving the advance notice).

c) this is governed by a contractual agreement in accordance with Art. 28(2-4) GDPR.

d) in cases where a subcontractor performs the agreed service outside of the EU/the EEA or Switzerland, BELLIN shall guarantee compliance with data protection provisions by means of relevant measures. The same applies if a service provider is to be commissioned pursuant to sentence 2 of Clause 6.1 of this DPA

For any subsequent outsourcing by subcontractors the following preconditions shall be met:

e) any subsequent outsourcing by subcontractors requires the express consent of BELLIN (at a minimum in text form), and

f) any and all contractual provisions in the contractual chain shall also apply to any additional contractors.

The transfer of personal data from the Customer by BELLIN to the subcontractor according to this Clause 6.3 and the subcontractor's commencement of the data processing shall only be undertaken once compliance with all preceding requirements has been achieved.

## 7. Audit Rights of the Customer

7.1 The Customer shall be entitled, in consultation with BELLIN, to conduct audits or to have them carried out by auditors to be appointed on a case-by-case basis at the Customer's expense according to the following provisions, to verify compliance with this DPA by BELLIN in its business operations. Any audits must be notified to BELLIN by the customer in good time.

7.2 BELLIN shall ensure that the Customer is able to verify BELLIN's compliance with obligations pursuant to Art. 28 GDPR. BELLIN obligates itself to provide the Customer with information required to uphold control of processors when requested by the Customer and to provide evidence in particular of technical and organizational measures as detailed in the schedule (TOM). BELLIN is entitled at its own discretion and considering the Customer's regulatory duties to withhold information that are sensitive to BELLIN's business or in case BELLIN would violate regulatory or other contractual obligations. The Customer is not entitled to have access to data or information about other customers of BELLIN, or information regarding service cost, or quality or contract management reports as well as any other confidential information of BELLIN that is not immediately related to the agreed purpose of the audit.

7.3 Evidence of compliance with such measures according to this specific DPA, may be demonstrated as follows at BELLIN's discretion:

a) Compliance with codes of conduct stipulated by Art. 40 GDPR;

b) Certifications obtained as part of an approved certification process pursuant to Art. 42 GDPR;

c) Current attestations, reports or report excerpts by independent bodies (e.g. auditors, audits, data protection officers, IT security departments, data protection auditors, quality auditors);

d) A suitable certification as part of an IT security or data protection audit (e.g. basic protection pursuant to BSI standards).

7.4 In case the Customer uses a third party for an audit the Customer shall ensure that the third party agrees to the same obligations towards BELLIN according to this section 7. In addition, the Customer has shall also ensure confidentiality and non-disclosure agreements by the third party unless the third party has professional confidentiality obligations. Upon request by BELLIN the Customer must provide to BELLIN such confidentiality agreements with that third party without undue delay. Competitors of BELLIN are not permitted to perform any audit for the Customer.

7.5 BELLIN shall be entitled to claim reasonable remuneration for enabling any audits conducted or commissioned by the Customer.

## 8. Reporting Violations by BELLIN

8.1 BELLIN shall support the Customer in their compliance efforts pursuant to Arts. 32 through 36 GDPR pertaining to the obligations to protect personal data, to report data breaches, to conduct data protection impact assessments and to ensure prior consultation. This includes:

a) The guarantee of an appropriate level of security by means of technical and organizational measures taking into account the context and purposes of processing and the predicted

likelihood and severity of a potential violation caused by security gaps and enabling the immediate identification of any relevant events constituting a violation.

b) The obligation to notify the Customer of any breach of personal data without delay.

c) The obligation to support the Customer in their statutory disclosure obligations towards data subjects and to provide them with any relevant information within this context without delay.

d) Support for the Customer with their data protection impact assessments.

e) Support for the Customer within the framework of prior consultations with regulatory authorities.

8.2 BELLIN shall be entitled to claim reasonable remuneration for any support services that exceed the service scope or where the misconduct cannot be attributed to BELLIN.

## 9. Customer Authority to Issue Instructions

9.1 Within the framework of the contractual scope set forth by this agreement, the Customer shall be entitled to make recommendations as to the nature, scope and methods of data processing and to put these in concrete terms by giving direct instructions. Any subsequent changes to the processing object or any changes to procedures shall then be agreed in writing, at least by email.

9.2 Data is solely handled within the scope of agreed provisions and per Customer instructions.

9.3 The Customer shall confirm any verbal instructions in writing, at least by email, prior to the implementation of these changes. BELLIN shall be obligated to notify the Customer without delay if they believe that an instruction violates data protection regulations. BELLIN shall be entitled to suspend the execution of the relevant instruction until it has been confirmed or amended by a Customer representative.

9.4 If arrangements made under this provision change, are canceled or amended, then this shall only be permitted if a corresponding new arrangement is made.

## 10. Deletion of Data and Return of Data Storage Devices

10.1 No data copies or duplicates shall be made without Customer's knowledge. This excludes backup copies provided these are required to ensure correct processing as well as data required to comply with statutory or governmental retention provisions.
Upon completion of contractually agreed work, or earlier if requested by the Customer, yet no later than upon expiry of this service agreement, BELLIN shall be obligated to return to the Customer all documents, data processing and usage reports in its possession as well as stored data which relates to the contractual relationship, or to destroy them in compliance with data protection provisions where prior consent has been obtained. The same applies to testing and scrap materials. A deletion protocol must be presented upon request.

10.2 Documentation that serves as proof of data having been processed properly and according to specifications shall be kept by BELLIN in accordance with applicable retention periods after the termination of the Contract. BELLIN may choose to pass on such documents to the Customer upon expiry of the Contract.

## 11. Liability

11.1 BELLIN'S liability is subject to the liability clause in the Contract with regard to liability exclusions and limitations. In case of claims by third parties against BELLIN which are based on a proven violation against this Contract or any of the Customer's duties as the responsible party with regard to data privacy, the Customer will hold BELLIN harmless from and against these claims upon first request

11.2 The Customers agrees to hold upon first request BELLIN harmless from any penalties claimed from BELLIN by a third party for which the Customer has responsibility for the violation that is sanctioned by such penalties.

## 12. Termination of the DPA

This DPA shall terminate immediately on the termination of the Contract between the Customer and BELLIN.

## SCHEDULE:
## GENERAL TECHNICAL AND ORGANIZATIONAL MEASURES (TOM) PURSUANT TO ART. 28 GDPR

This schedule describes the technical and organizational measures undertaken by BELLIN.

# 1. Confidentiality (Art. 32(1)(b) GDPR)

- Physical access control

  There is a general access control system using card readers, monitoring systems and controlled key distribution.

  The following applies to any premises used by BELLIN:

  - Burglar alarm system including 24/7 alarm generation to a security company
  - Magnetic and closing contacts on all exterior and partitioning interior doors, as well as for admission to particularly sensitive areas such as server rooms.
  - Keyless access with magnetic cards and person-based authorizations
  - Biometric access barriers
  - Manual locking system
  - Locking system with code lock
  - Extensive logs for the use of access cards
  - Video surveillance of buildings and entrances
  - Secured building shafts
  - Doors with external door knobs
  - Video entry system
  - Key control policy/list
  - Staffed entrance or reception/security staff at entrance
  - Visitor book/visitor log
  - Employee/visitor passes
  - Visitors accompanied by employees
  - Careful selection of security guards
  - Careful selection of cleaning staff

  The following also applies to the data center used:

  Access to the data center is protected by state-of-the-art security devices, and entry is logged. The group of persons with access authorization is limited. A general fire, burglary and leak protection system is installed.

  - Security locks, key cards
  - Visual inspection by the data center staff
  - CCTV video surveillance, security alarm
  - 24x7x365: Personnel in buildings, technical support

- System access control
  The intrusion of unauthorized persons into the IT systems is prevented. Strong passwords are in use, which are changed regularly, and user management together with user identification and authentication is in effect.
  - Login with username and password
  - Login with biometric data
  - Antivirus software installed on the servers
  - Antivirus software installed on the clients
  - Firewall
  - Intrusion detection systems
  - Remote access takes place only over encrypted lines (VPN).
  - Encryption of data storage devices
  - Encryption of notebooks/tablets
  - Management of user permissions
  - Central assignment of passwords
  - "Secure password" policy
  - "Deletion/destruction" policy
  - "Clean desk" policy
  - General data protection and/or security policy
  - Mobile device policy
  - Instructions for staff on how to manually lock desktops
  - Restrictive access control applies to server rooms
- Data access control
  - Confidential or highly confidential paper documents are locked away securely or disposed of properly (shredder)
  - Well-defined employee authorizations with access permissions to the servers
  - Physical deletion (secure sanitization) of data storage devices
  - Logging of access to applications, specifically when data is entered, altered and deleted; software-controlled logging of access to servers with critical data
  - Number of administrators kept to the minimum necessary
  - Management of user rights by administrators
  - A security safe
  - Unauthorized activities in computer systems that go beyond authorized access are prevented. Restrictive, needs-based authorization concepts are applied. Access authorizations are monitored and logged. Users are trained in privacy policy and application use. Limited and documented data access
  - Regular training and mandatory sessions for all employees on the handling of sensitive data and data security

- Separate processing control
  Data collected for different purposes shall be processed separately. Different customers' data shall not be processed together.
  - Separation between server operation and application development
  - Processes and applications shall be separated in the organization as follows
    - Development
    - BELLIN Cloud services
    - Support
  - Physical separation (systems/databases/data storage devices)
  - Multi-client applications used where relevant: different customers' data is stored in different databases. Data is collected and processed in customer-specific applications.
  - Control via user permissions model
  - Specification of database rights
  - Data records have purpose attributes
- Pseudonymization (Art. 32(1)(a) GDPR; Art. 25(1) GDPR)
  Where personal data is pseudonymized, it is processed in such a way that no data may be matched to a specific data subject without additional information. Where pseudonymization is used, additional information for attributing the personal data to a specific data subject is kept separately in separate and secure systems. There is an internal requirement to anonymize/pseudonymize personal data as far as possible where the data is to be transmitted or the statutory time limit for deletion of data expires.

## 2. Integrity (Art. 32(1)(b) GDPR)

- Data transmission control
  - Email encryption
  - Use of VPNs
  - Logging of access and retrieval
  - Use of encrypted connections such as sftp/https for transmission
  - Transmission of data in anonymized or pseudonymized form
  - The electronic transfer of data and transmission of personal data is carried out with state-of-the-art encryption methods. Data is only disclosed in predetermined channels according to the technical requirements of the banks to which the data is to be transmitted.
  - Data is stored exclusively in the framework of legal requirements and tax regulations.
  - Data will only be transmitted via insecure channels (e.g. by email) after BELLIN has been expressly instructed to do so by the Customer.
- Input control
  - The traceability and documentation of data management and maintenance is ensured at the level of individual usernames (not user groups) by the audit trail. Data input is performed exclusively by the Customer, the role of BELLIN is data transmission.
  - The readability of the data is controlled by the application.
  - Data processing outside of the application is controlled by the Customer and only possible under clearly defined exceptional circumstances, requiring a written instruction by the Customer.
  - Clear responsibilities for deleting data

## 3. Availability and Resilience (Art. 32(1)(b) GDPR)

- Availability control and ability to quickly restore data
  - Fire and smoke detection systems
  - Fire extinguishers in server rooms
  - Devices for monitoring temperature and humidity in server rooms
  - Air conditioning in server rooms
  - Uninterruptible power supplies (UPSs)
  - Sockets with protective contacts in server room power strips
  - RAID system/hard disk mirroring
  - Video surveillance of server rooms
  - Alarm notification in case of unauthorized access to server rooms
  - Data shall be protected against accidental destruction or loss. An emergency plan is in place, including backup processes and decentralized data storage. There are defined availability periods.
  - The redundant servers are available in two different data centers, which are connected by a fiber path to form a VLAN
  - Backups are regularly available as agreed; a backup and recovery plan is in place
  - Monitoring of the backup process
  - Regular tests in relation to data recovery and logging of results
  - Storage of the backup media in a secure location outside of server rooms
  - No sanitary installations located in or above server rooms
  - Separate partitions for operating systems and data
  - Servers at redundant locations
  - Computer and storage media in use is subject to active monitoring 24/7

## 4. Procedures for Regular Audits, Assessments and Evaluations (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

- Data protection management
  - Software solution is used
  - Central record kept of all data protection procedures and rules with access for employees based on need/authorization
  - ISO 27001 security certification
  - A review of the effectiveness of technical protection measures is carried out at least once a year
  - External data protection officer
  - Employees trained and required to maintain confidentiality/data secrecy
  - Regular awareness-raising activities for employees, at least once a year
  - Internal information security officer
  - Data Protection Impact Assessment (DPIA) is carried out if necessary
  - The organization complies with its obligations to provide the information referred to in Articles 13 and 14 of the GDPR
  - Formalized process is in place for dealing with requests by data subjects to access their personal data
- Incident response management
  - Use of firewall with regular updates
  - Use of spam filter with regular updates
  - Use of virus scanner with regular updates
  - Intrusion detection system (IDS)
  - Intrusion prevention system (IPS)
  - Documented process for identifying and reporting security incidents/data breaches (which also covers the obligation to notify the supervisory authorities)
  - Involvement of data protection officer and information security officer in security incidents and data breaches
  - Recording of security incidents and data breaches e.g. via ticketing system
  - Formal process and responsibilities for following up security incidents and data breaches
- Data protection by default (Art. 25(2) GDPR)
  - Only personal data which is necessary for each specific purpose is collected
  - Technical measures are in place which enable data subjects to easily exercise their right to withdraw consent
- Control of processors
  - No data is processed by processors on behalf of the controller within the meaning of Art. 28 of the GDPR without corresponding instruction by the Customer
  - Prior examination of the security measures taken by the processor and recording of these measures
  - Due diligence carried out when selecting the processor (especially in relation to data protection and data security)
  - The necessary agreement for processors is entered into or EU standard contractual clauses are used
  - The processor's staff are required to maintain data secrecy
  - The processor is required to appoint a data protection officer where there is a legal obligation to do so
  - Agreement of effective monitoring rights with respect to the processor

- Rules for the use of sub-processors (subcontractors)
- Procedures are in place to ensure data is destroyed after the processing on behalf of the controller is completed
- In the case of prolonged collaboration with the processor, the level of data protection provided by the processor is reviewed on an ongoing basis