



PERSONAL DATA PROCESSING AGREEMENT FOR CORESYSTEMS SERVICES

1. BACKGROUND

1.1 Purpose.

This document is a data processing agreement (“DPA”) between CORESYSTEMS and Customer and applies to Personal Data provided by Customer and each Data Controller in connection with their use of the CORESYSTEMS Services. It states the technical and organizational measures CORESYSTEMS uses to protect Personal Data that is stored in the production system of CORESYSTEMS Services.

1.2 Application of the Standard Contractual Clauses Document.

If processing of Personal Data involves an International Transfer, the Standard Contractual Clauses apply as stated in Section 5 and are incorporated by reference.

1.3 Governance.

Except as provided in Section 5.2, Customer is solely responsible for administration of all requests from other Data Controllers. Customer will bind any other Data Controller it permits to use CORESYSTEMS Services to the terms of this DPA.

2. APPENDICES

Customer and its Data Controllers determine the purposes of collecting and processing Personal Data in CORESYSTEMS Services. Appendix 1 states the details of the processing CORESYSTEMS will provide via its Services. Appendix 2 states the technical and organizational measures CORESYSTEMS applies to the its Services, unless the Agreement states otherwise.

3. CORESYSTEMS OBLIGATIONS

3.1 Instructions from Customer.

CORESYSTEMS will follow instructions received from Customer (on its own behalf or on behalf of its Data Controllers) with respect to Personal Data, unless they are (i) legally prohibited or (ii) require material changes to CORESYSTEMS Services. CORESYSTEMS may correct or remove any Personal Data in accordance with the Customer’s instruction. If CORESYSTEMS cannot comply with an instruction, it will promptly notify Customer (email permitted).

3.2 Data Secrecy.

To process Personal Data, CORESYSTEMS and its Subprocessors will only use personnel who are bound to observe data and telecommunications secrecy under the Data Protection Law. CORESYSTEMS and its Subprocessors will regularly train individuals having access to Personal Data in data security and data privacy measures.

3.3 Technical and Organizational Measures.

(a) CORESYSTEMS will use the appropriate technical and organizational measures stated in [Appendix 2](#).

(b) Appendix 2 applies to all the Services provided by CORESYSTEMS on production environments. Customer should not store any Personal Data in non-production environments.

(c) CORESYSTEMS provides its Services to CORESYSTEMS’s entire customer base hosted out of the same data centers and receiving the same Service. Customer agrees CORESYSTEMS may improve the measures taken in Appendix 2 in protecting Personal Data so long as it does not diminish the level of data protection.

3.4 Security Breach Notification.

CORESYSTEMS will promptly inform Customer if it becomes aware of any Security Breach.

3.5 Cooperation.

At Customer’s request, CORESYSTEMS will reasonably support Customer or any Data Controller in dealing with requests from Data Subjects or regulatory authorities regarding CORESYSTEMS’s processing of Personal Data.

4. SUBPROCESSORS

4.1 Permitted Use.

(a) Customer and Data Controllers authorize CORESYSTEMS to subcontract the processing of Personal Data to Subprocessors. CORESYSTEMS is responsible for any breaches of the Agreement caused by its Subprocessors.

(b) Subprocessors will have the same obligations as CORESYSTEMS does as a Data Processor (or Subprocessor) with regard to their processing of Personal Data.

(c) CORESYSTEMS will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection. Subprocessors may have security certifications that evidence their use of appropriate security measures. If not, CORESYSTEMS will regularly evaluate each Subprocessors security practices as they relate to data handling.

(d) CORESYSTEMS will inform Customer of the name, address and role of each Subprocessor it uses to provide its Services. Subprocessors are:

- Coresystems FSM, AG
- Microsoft, Inc (Skype 4 Business, Office 365, Azure)
- Atlassian, Inc (Confluence) will be replaced by Wiki
- Git, Inc
- SAP, SE (SAP Business One, C/4HANA Service Cloud)
- Peral, Inc
- Zendesk, Inc
- Redmine, Inc
- Slack, Inc
- Envoy, Inc
- Cyon, Inc

4.2 New Subprocessors.

CORESYSTEMS's use of Subprocessors is at its discretion, provided that:

(a) CORESYSTEMS will notify Customer in advance (by email or by posting on the Support Portal) of any changes to the list of Subprocessors in place on the Effective Date (except for Emergency Replacements or deletions of Subprocessors without replacement).

(b) If Customer has a legitimate reason that relates to the Subprocessors processing of Personal Data, Customer may object to CORESYSTEMS's use of a Subprocessor, by notifying CORESYSTEMS in writing within thirty days after receipt of CORESYSTEMS's notice. If Customer objects to the use of the Subprocessor, the parties will come together in good faith to discuss a resolution. CORESYSTEMS may choose to: (i) not use the Subprocessor or (ii) take the corrective steps requested by Customer in its objection and use the Subprocessor. If none of these options are reasonably possible and Customer continues to object for a legitimate reason, either party may terminate the Agreement on thirty days' written notice. If Customer does not object within thirty days of receipt of the notice, Customer is deemed to have accepted the new Subprocessor.

(c) If Customer's objection remains unresolved sixty days after it was raised, and CORESYSTEMS has not received any notice of termination, Customer is deemed to accept the Subprocessor.

4.3 Emergency Replacement.

CORESYSTEMS may change a Subprocessor where the reason for the change is outside of CORESYSTEMS's reasonable control. In this case, CORESYSTEMS will inform Customer of the replacement Subprocessor as soon as possible. Customer retains its right to object to a replacement Subprocessor under Section 4.2(b).

5. INTERNATIONAL TRANSFERS

5.1 Limitations on International Transfer.

Personal Data from an EEA or Swiss Data Controller(s) may only be exported or accessed by CORESYSTEMS or its Subprocessors outside the EEA or Switzerland ("**International Transfer**"):

(a) If the recipient, or the country or territory in which it processes or accesses Personal Data, ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data as determined by the European Commission; or

(b) in accordance with Section 5.2.

5.2 Standard Contractual Clauses and Multi-tier Framework.

(a) The Standard Contractual Clauses apply where there is an International Transfer to a country that does not ensure an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data as determined by the European Commission.

(b) For Third Country Subprocessors, CORESYSTEMS has entered the unchanged version of the Standard Contractual Clauses prior to the Subprocessors processing of Personal Data. Customer hereby (itself as well as on behalf of each Data Controller) accedes to the Standard Contractual Clauses between CORESYSTEMS and the Third Country Subprocessor. CORESYSTEMS will enforce the Standard Contractual Clauses against the Subprocessor on behalf of the Data Controller if a direct enforcement right is not available under Data Protection Law.

(c) Nothing in this DPA will be construed to prevail over any conflicting clause of the Standard Contractual Clauses.

6. CERTIFICATIONS AND AUDITS

6.1 Customer Audits.

Customer or its independent third-party auditor may audit CORESYSTEMS's control environment and security practices relevant to Personal Data processed by CORESYSTEMS only if:

(a) CORESYSTEMS has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the provided services through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 attestation report. Upon Customer's request -SOC Audit reports or ISO certifications are available through the third-party auditor;

(b) A Security Breach has occurred;

(c) Customer or another Data Controller has reasonable grounds to suspect that CORESYSTEMS is not in compliance with its obligations under this DPA;

(d) An audit is formally requested by Customer's or another Data Controller's data protection authority; or

(e) Mandatory Data Protection Law provides Customer with a direct audit right.

Where Customer audits CORESYSTEMS's environment, CORESYSTEMS will reasonably support Customer in its audit processes.

6.2 Audit Restrictions.

The Customer audit will be limited to once in any twelve months period, and limited in time to a maximum of 3 business days and scope as reasonably agreed in advance between the parties. Reasonable advance notice of at least sixty days is required, unless Data Protection Law requires earlier audit. CORESYSTEMS and Customer will use current certifications or other audit reports to minimize repetitive audits. Customer and CORESYSTEMS will each bear their own expenses of audit, unless the Customer is auditing under Section 6.1 (c) (unless such audit reveals a breach by CORESYSTEMS in which case CORESYSTEMS shall bear its own expenses of audit), 6.1 (d) or 6.1 (e). In those cases, Customer will bear its own expense and the cost of CORESYSTEMS's internal resources required to conduct the audit. If an audit determines that CORESYSTEMS has breached its obligations under the Agreement, CORESYSTEMS will promptly remedy the breach at its own cost.

7. EU ACCESS

7.1 Optional Service.

If included in the Order Form, CORESYSTEMS agrees to provide EU Access for the eligible Services as stated in this Section 7.

7.2 EU Access.

CORESYSTEMS will use only European Subprocessors to provide support requiring access to Personal Data.

7.3 Data Center Location.

Upon the Order Form Effective Date, the Data Centers used to host Personal Data are located in the EEA or Switzerland. CORESYSTEMS will not migrate the Customer instance to a Data Center outside the EEA or Switzerland without Customer's prior written consent (email permitted). If CORESYSTEMS plans to migrate the Customer instance to a data center within the EEA or to Switzerland, CORESYSTEMS will notify Customer in writing (email permitted) no later than thirty days before the planned migration.

7.4 Exclusions.

The following Personal Data is not subject to the requirements in 7.2-7.3:

- (a) Contact details of the sender of a support ticket;
- (b) Any other Personal Data submitted by Customer when filing a support ticket. Customer may choose not to transmit Personal Data when filing a support ticket. If this data is necessary for the incident management process, Customer may choose to anonymize that Personal Data before any transmission of the incident message to CORESYSTEMS;
- (c) Personal Data in non-production systems.

8. DEFINITIONS

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

8.1 “Data Center” means the location where the production instance of the Service is hosted for the Customer in its region, as agreed in an Order Form.

8.2 “Data Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

8.3 “Data Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

8.4 “Data Protection Law” means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

8.5 “Data Subject” means an identified or identifiable natural person.

8.6 “EEA” means the European Economic Area, namely the European Union Member States along with Iceland, Lichtenstein and Norway.

8.7 “European Subprocessor” means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland.

8.8 “Personal Data” means any information relating to a Data Subject For the purposes of this DPA, it includes only personal data entered by Customer or its Authorized Users into or derived from their use of CORESYSTEMS Services. It also includes personal data supplied to or accessed by CORESYSTEMS or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data.

8.9 “Security Breach” means a confirmed (1) accidental or unlawful destruction, loss, alteration, or disclosure of Customer Personal Data or Confidential Data, or (2) similar incident involving Personal Data for which a Data Processor is required under applicable law to provide notice to the Data Controller.

8.10 “Standard Contractual Clauses” or sometimes also referred to the “EU Model Clauses” means the (Standard Contractual Clauses (processors)) or any subsequent version thereof released by the Commission (which will automatically apply). The current Standard Contractual Clauses are located at http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc. They include Appendices 1 and 2 attached to this DPA.

8.11 “Subprocessor” means CORESYSTEMS Affiliates and third parties engaged by CORESYSTEMS or CORESYSTEMS’s Affiliates to process personal data.

8.12 “Third Country Subprocessor” means any Subprocessor incorporated outside the EEA and outside any country for which the European Commission has published an adequacy decision as published at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

Appendix 1 to Data processing agreement and Standard Contractual Clauses

Data Exporter

The Data Exporter subscribed to a Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data.

Data Importer

CORESYSTEMS and its Subprocessors provide the Services that includes the following support:

CORESYSTEMS Affiliates support the data centers remotely from CORESYSTEMS facilities in Windisch (Switzerland), and other locations where CORESYSTEMS employs personnel in the Operations/Cloud Delivery function. Support includes:

- Monitoring the Services
- Backup & restoration of Customer Data
- Release and development of fixes and upgrades to the provided Services
- Monitoring, troubleshooting and administering the underlying Service infrastructure and database
- Security monitoring, network-based intrusion detection support, penetration testing

CORESYSTEMS Affiliates provide support when a Customer submits a support ticket because the Service is not available or not working as expected for some or all Authorized Users. CORESYSTEMS answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Service.

Data Subjects

Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of data subjects: employees, contractors, business partners or other individuals having Personal Data.

Data Categories

The transferred Personal Data concerns the following categories of data:

name, phone numbers, e- mail address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users enter the Service and may include bank account data, credit or debit card data.

Special Data Categories (if appropriate)

The transferred Personal Data concerns the following special categories of data: As set out in the Order Form, if any.

Processing Operations

The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Service (including Operational and Technical Support)
- provision of Consulting Services;
- communication to Authorized Users
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- upload any fixes or upgrades to the Services
- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with this Agreement

Appendix 2 – Technical and Organizational Measures

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define the CORESYSTEMS's current security measures. CORESYSTEMS may change these at any time without notice so long as it maintains a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

1.1 Physical Access Control.

Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- CORESYSTEMS protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.
- In general, buildings are secured through access control systems.
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to CORESYSTEMS buildings must register their names at reception and must be accompanied by authorized CORESYSTEMS personnel.

• CORESYSTEMS employees and external personnel must wear their ID cards at all CORESYSTEMS locations. Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To ensure proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
- CORESYSTEMS and all third-party Data Center providers log the names and times of persons entering CORESYSTEMS's private areas within the Data Centers.

1.2 System Access Control.

Data processing systems used to provide the CORESYSTEMS Services must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.
- All users access CORESYSTEMS's systems with a unique identifier (user ID).
- CORESYSTEMS has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, his or her access rights are revoked.
- CORESYSTEMS has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- CORESYSTEMS uses up-to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.

- Security patch management is implemented to ensure regular and periodic deployment of relevant security updates.
- Full remote access to CORESYSTEMS's corporate network and critical infrastructure is protected by strong authentication.

1.3 Data Access Control.

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

- As part of the CORESYSTEMS Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the CORESYSTEMS Information Classification standard.
- Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. CORESYSTEMS uses authorization concepts that document how authorizations are assigned and which authorizations are assigned to whom. All personal, confidential, or otherwise sensitive data is protected in accordance with the CORESYSTEMS security policies and standards. Confidential information must be processed confidentially.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, CORESYSTEMS conducts internal and external security checks and penetration tests on its IT systems.
- CORESYSTEMS does not allow the installation of personal software or other software that has not been approved by CORESYSTEMS.
- An CORESYSTEMS security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control.

Except as necessary for the provision of the Services in accordance with the relevant service agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at CORESYSTEMS to ensure the agreed-upon service levels (for example, encryption and lead-lined containers).

- Personal Data transfer over CORESYSTEMS internal networks are protected in the same manner as any other confidential data according to CORESYSTEMS Security Policy.
- When data is transferred between CORESYSTEMS and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant Agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of CORESYSTEMS-controlled systems (e.g. data being transmitted outside the firewall of the CORESYSTEMS Data Center).

1.5 Data Input Control.

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from CORESYSTEMS data processing systems.

Measures:

- CORESYSTEMS only allows authorized persons to access Personal Data as required in the course of their work.
- CORESYSTEMS has implemented a logging system for input, modification and deletion, or blocking of Personal Data by CORESYSTEMS or its Subprocessors within CORESYSTEMS's Products and Services to the fullest extent possible.

1.6 Job Control.

Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the relevant agreement and related instructions of the customer. Measures:

- CORESYSTEMS uses controls and processes to ensure compliance with contracts between CORESYSTEMS and its customers, Subprocessors or other service providers.
- As part of the CORESYSTEMS Security Policy, Personal Data requires at least the same protection level as “confidential” information according to the CORESYSTEMS Information Classification standard.
- All CORESYSTEMS employees and contractual Subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of CORESYSTEMS customers and partners.
- For on premise support services, CORESYSTEMS provides a specially designated, secure support ticket facility in which CORESYSTEMS provides a special access-controlled and monitored security area for transferring access data and passwords. CORESYSTEMS customers have control over their remote support connections at all times. CORESYSTEMS employees cannot access a customer system without the knowledge or full active participation of the customer.

1.7 Availability Control.

Personal Data will be protected against accidental or unauthorized destruction or loss. Measures:

- CORESYSTEMS employs backup processes and other measures that ensure rapid restoration of business-critical systems as and when necessary.
- CORESYSTEMS uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the Data Centers.
- CORESYSTEMS has defined contingency plans as well as business and disaster recovery strategies for the provided Services.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control.

Personal Data collected for different purposes can be processed separately. Measures:

- CORESYSTEMS uses the technical capabilities of the deployed software (for example: multi-tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customers (including their Affiliates) have access only to their own data.
- If Personal Data is required to handle a support incident from a specific customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

1.9 Data Integrity Control.

Personal Data will remain intact, complete and current during processing activities. Measures:

CORESYSTEMS has implemented a multi-layered defense strategy as a protection against unauthorized modifications. In particular, CORESYSTEMS uses the following to implement the control and measure sections described above. In particular:

- Firewalls;
- Security Monitoring Center;
- Backup and recovery;
- Internal penetration testing;