concrefy

FRESH THINKING
FOR CONSTRUCTION

DATA PROCESSING AGREEMENT (DPA)

1. GENERAL

1.1. This Data Processing Agreement ("DPA") governs the rights and obligations of Concrefy as processor and the client/Customer as data controller in connection with the processing of personal data on behalf of Concrefy.

1.2. This DPA applies to all activities where the processor or authorized subcontractors (sub-processors) process personal data of the client.

1.3. Terms used in this DPA should be understood in accordance with their definition in the EU General Data Protection Regulation (GDPR).

1.4. The provisions of this DPA are in accordance with the **Algemene Verordening Gegevensbescherming (AVG)**, the Dutch implementation of the GDPR. Where this agreement refers to the GDPR, this shall be deemed to also refer to the corresponding provisions of the AVG.

2. CONTENT OF THE PROCESSING

2.1. The processing is based on the agreement concluded between the parties (Quotation and Concrefy General Terms and Conditions) pursuant to which the Processor provides to the Client certain services consisting of software applications, web portals and related support components such as consulting, testing or maintenance (the 'Agreement'). In this context, the Processor will process personal data of Authorized Users/Users (typically employees of the Customer), as well as other natural persons involved in the operational processes of the Customer, such as employees of construction companies, subcontractors, architects, suppliers, production partners or other third parties designated by the Customer or whose data is uploaded by the Processor as a data controller, for the purpose of providing and delivering the Concrefy solutions and services/services.

2.2. The following data categories are processed for the benefit of the Controller: Name, contact information (such as email address, phone numbers, etc), contract information, login information (username and password), log information (date and time), selected operating device, company, affiliation and function in the company, location, role in the service, preferred language, logs (images), data when requesting support services (e.g. "tickets").

2.3. Data entered into the service for testing, testing reports, construction projects and Customer construction sites, measurement data, inventory data, material composition data, item master data, financial data, order data, are not covered by this DPA

2.4. The purpose of processing personal data is the performance of the work specified solutions in the main contract as services, services, performance or Concrefy or for which the Customer has subsequently given instructions to the processor.

2.5. The duration of the processing is governed by the provisions of the main agreement, where further obligations may arise from legal provisions.

3. RIGHTS AND OBLIGATIONS OF THE PROCESSOR.

3.1. The Processor shall process the Personal Data solely on the basis of the Main Agreement, this DPA and the Customer's documented instructions - including with respect to the transfer of Personal Data to a third country or an international organization - unless the Processor is required to do so by Union law or Member State law to which the Processor is subject, in which case the Processor shall notify the Customer of such legal requirements prior to the processing , unless the relevant law prohibits such notification on the grounds of substantial public interest.

3.2. The Processor guarantees that the persons authorized to process the Personal Data have committed to confidentiality or are subject to an appropriate legal obligation of confidentiality.

3.3. The Processor shall take all measures within its sphere of influence in accordance with Article 32 GDPR (see the Annex 1 to this DPA). These measures depend on technical progress and the state of the art. Minor developments will be implemented without consulting the Customer.

3.4. The Customer authorizes the Processor to use sub-processors (in particular IT service providers). Care must be taken to ensure that the sub-processor undertakes the same obligations that are incumbent on the Processor under this Agreement. If the sub-processor fails to fulfill its data protection obligations, the Processor shall be liable to the Customer for the fulfillment of the sub-processor's obligations.

3.5. The sub-processors placed in particular https://www.concrefy.com/sub-processors are subject to the general authorization in accordance with Section 3.4.

3.6. The Processor undertakes to transfer personal data outside the European Economic Area only if appropriate safeguards for compliance with applicable data protection legislation (e.g. conclusion of model contractual clauses) have been provided.

3.7. The Processor shall notify the Customer at least seven (7) days prior to the engagement of a new or replacement of an existing sub-processor, whereby - at the sole discretion of the Processor - (i) an email to the Customer; or (ii) publication on the Customer portal or Customer platform; or (iii) publication onhttps://www.concrefy.com/sub-processors is sufficient, and hereby grants Customer the right to object to the engagement of a new or replacement of an existing sub-processor, provided that such sub-processor demonstrably does not ensure the same or a reasonably comparable level of protection for the processing of personal data. The Customer's objection constitutes good cause for the processor to terminate the contract within the meaning of the contractual terms. An objection from the Customer that does not meet the above requirements is irrelevant.

3.8. Given the nature of the processing, the Processor shall, where possible, support the Customer with appropriate technical and organizational measures to comply with its obligation to respond to requests to exercise the data subject's rights referred to in Chapter III GDPR. If the data subject contacts the Processor directly, the Processor will refer them to the Customer. This is provided that the Processor is able to correlate the data subject with the Customer based on the information provided by the data subject. The Processor is not liable in cases where the Customer does not respond fully, correctly or in a timely manner to the Data Subject's request.

3.9. The Processor shall completely anonymize or erase all personal data within a period of one hundred and eighty (180) days after the termination of the provision of processing services, unless there is an obligation to retain the personal data under Union or Member State law or the data is necessary for the establishment, exercise or defense of legal claims.

3.10. Prior to anonymization or erasure, the Customer may receive the personal data in a commonly used electronic format chosen by the Processor for a reasonable fee.

3.11. The Processor shall, taking into account the nature of the processing and the information available to the Processor, assist the Customer in complying with the obligations of Articles 32 to 36 GDPR.

3.12. The Processor shall provide the Customer with all information necessary to demonstrate compliance with the obligations of this DPA and shall perform and contribute to audits in accordance with Section 4.5 of this GDPR. However, the Customer agrees that audits in accordance with Section 4.5 may be replaced at discretion of the Processor by providing detailed documentation of the implemented data protection and security measures, relevant certifications or reports of external auditors.

3.13. The Processor must immediately notify the Customer if it believes that any specific instruction given by the Customer violates applicable data protection regulations.

4. RIGHTS AND OBLIGATIONS OF THE CUSTOMER

4.1. The Customer is solely responsible for assessing the permissibility of the instructed processing and for safeguarding the rights of data subjects and for making the necessary notifications to the Processor. The Customer shall inform the Processor of the contact point for all questions arising from or related to this DPA.

4.2. The Customer shall provide all assignments, partial assignments or instructions that differ from or supplement the main agreement in writing. In urgent cases, instructions may be given orally. Customer shall promptly confirm such instructions in writing.

4.3. The Customer shall immediately inform the processor if it finds errors or irregularities in the examination of order results.

4.4. The Customer shall not process special categories of personal data without the written consent of the processor. Customer will not process data of persons under 14 years of age.

4.5. Subject to Section 3.12 of this DPA, the Customer shall have the right to verify compliance with the obligations set forth in this DPA itself or through third parties who are contractually or legally bound to confidentiality and who are not competitors of the Processor and its affiliates, on-site. The Customer or a third party authorized by the Customer shall comply with the Processor's internal security requirements (in particular in accordance with applicable security and IT guidelines) in the context of such controls. Due to confidentiality or security requirements, on-site controls of certain environments and information (e.g. to compromise the rights of third parties or to protect trade secrets) may be restricted to the extent necessary. Environments not relevant to the obligations in this DPA are expressly excluded from the Customer's right of inspection.

4.6. The Customer shall bear the costs of such inspection. Inspections must be conducted without disrupting business operations and during general business hours. Unless otherwise indicated for urgent reasons to be documented by the Customer, inspections shall take place after reasonable advance notice (of at least 30 business days), if possible for up to one day on a mutually agreed schedule that minimizes the impact of the audit on the processor's operations, and no more frequently than every 12 months.

5. FINAL PROVISIONS

5.1. Amendments and supplements to this DPA must be in writing and must be expressly identified as such.

5.2. Should individual provisions of this DPA be or later become invalid or unenforceable, this shall not affect the validity of the remainder of the Data Protection Agreement. The parties undertake to replace such provision with a valid one. The same applies in the event of a contractual loophole.

5.3. Dutch substantive law shall apply to the exclusion of conflict of laws and the UN Convention on Contracts for the International Sale of Goods.

5.4. The German and English language versions of this Data Processing Agreement are provided for information purposes. Only the Dutch language version is binding between the parties.

Annex 1 -Technical and Organizational Measures according to Art. 32 GDPR

Confidential (Art. 32 para. 1 lit. b GDPR)

a) Access Control.

The following implemented measures prevent unauthorized access to data processing facilities:

	implemented
Access control system, card reader (magnetic/chip card)	✓
Door security (electric door opener, combination lock, etc.)	✓
Secured doors/windows	✓
Fence systems	✓
Key management, documentation of key assignment	✓
Factory security, doorman, security service	✓
Alarm system	✓
Special protective measures for storage of backups and/or other data media	✓
Non-reversible destruction of data carriers	✓
Staff and authorization badges	✓
Lockable sections	✓
Visitor regulations (e.g., pick up at reception, documentation of visiting hours, visitor badge, escort after visit to exit)	✓

b) Access control

The following implemented measures prevent unauthorized access to data processing systems:

	implemented
Personal and individual user login when logging into the system or company network	✓
Authorization process for access rights	✓
Restriction of authorized users	✓
One-time login	✓
Password policy (specification of password DPArameters in terms of complexity and update interval, password history)	✓
Electronic documentation of passwords and protection of this documentation from unauthorized access	✓
Registration of access to the system	✓
Additional system login for certain applications	✓
Automatic locking of clients after a certain period without user activity (also password protected screensaver or automatic pause)	✓
Up-to-date firewall	✓
Updated antivirus software	✓

c) Access control

The following implemented measures ensure that unauthorized persons do not have access to personal data:

	Implemented
Central management and documentation of authorizations	✓
Conclusion of data processing contracts for the remote maintenance of data processing systems, provided that the remote maintenance involves the processing of PII, i.e. the processing of personal data, as part of the service.	✓
Authorization process for permissions.	✓
Authorization routines	✓
Profiles/roles	
Encryption of hard drives and/or laptops	✓
Process of segregation of duties	✓
Non-reversible deletion of data carriers	✓
Privacy screens for mobile data processing systems	✓
Patch management	✓

(d) Control of segregation

The following measures ensure that personal data collected for different purposes are processed separately.

	implemented
Storage of data records in separate databases	✓
Processing on separate systems	✓
Access authorizations according to functional responsibility	✓
Multi-client capability of IT systems	✓
Use of test data	✓
Separation of development and production environments	✓
Authorization concept	✓
Network segmentation	✓

Integrity (Art. 32 para. 1 lit. b GDPR)

a) Disclosure control

It shall be ensured that personal data cannot be read, copied, modified or deleted without authorization during transmission or storage on data carriers and that it is possible to verify which persons or bodies have received personal data. The following measures shall be implemented to ensure this:

	implemented
Encryption of the storage medium of laptops	✓
Secure file transfer (collaboration, Sharepoint)	✓
Secure data transport (e.g. TLS)	✓
Electronic signature	✓
Secure WLAN	✓
Regulation for handling mobile storage media (e.g. laptops, USB stick, cell phone)	✓
Remote tunneled data connections (VPN = Virtual Private Network)	✓
Classification of data	✓

(b) Input control

The following measures ensure that it is possible to control who has processed personal data in data processing systems and at what time:

	implemented
Access rights	✓
Document management system (DMS) with change history	✓
Functional responsibilities, organizationally defined responsibilities	✓

Availability and resilience (Art. 32 para. 1 lit. b GDPR)

Control of availability and resilience

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the Customer:

	implemented
Established backup procedure	✓
Storage process for backups (e.g. fireproof safe, separate fire compartment).	✓
Ensure data storage in secure network	✓
Install security updates as needed	✓
Mirroring of hard drives	✓
Installation of an uninterruptible power supply (UPS)	✓
Appropriate filing space for paper documents	✓
Fire and/or fire water protection of the server room	✓
Fire and/or fire water protection of the archive rooms	✓
Server room with air conditioning	✓
Protection against viruses	✓
Firewall	✓
Redundant, locally separated data storage (offsite storage)	✓
Monitoring of all relevant servers	✓
Backup data center	✓
Critical components are redundant	✓

Procedure for periodic review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

a) Data protection management

The following measures are designed to ensure that there is an organization that meets the basic requirements of the data protection legislation:

	implemented
Data protection policy (protection of PII).	✓
Establishment of a data protection committee	✓
Obligation of employees to maintain data confidentiality	✓
Maintaining an overview of processing activities (Art. 30 GDPR)	✓
Software solution for data protection management in use	✓
Certification according to ISO 9001	✓
Standardized process for handling information requests and other rights of data subjects	✓
Central documentation of all data protection procedures and regulations with access for employees based on authorization	✓

b) Incident management

The following measures are designed to ensure that notification processes are initiated in the event of data protection breaches:

	implemented
Notification process for data protection violations according to para. 4 No. 12 GDPR with respect to the supervisory authorities (Art. 33 GDPR)	✓
Notification process for data protection violations according to para. 4 No. 12 GDPR with respect to the data subjects (Art. 34 GDPR)	✓
Documented procedure for handling security incidents	✓

c) Privacy-friendly default settings (Art. 25 para. 2 GDPR)

Standardized default settings of systems and apps as well as data processing procedures must be taken into account. At this stage, functions and rights are concretely configured, the permissibility or impermissibility of certain inputs or input options (e.g. free texts) are defined with respect to data minimization, and decisions are made regarding the availability of user functions (e.g. with respect to the scope of processing). The type and scope of personal referencing or anonymization (e.g. in the case of selection, export and evaluation functions, which may be specified and made available by default or freely configurable) or the availability of certain processing functions, logging, etc. are also specified.

	implemented
Mark input fields in online forms as mandatory fields only if absolutely necessary for the further process.	✓
Easy exercise of the right of withdrawal via technical measures (e-mail footer).	✓

d) Order control

The following measures ensure that personal data can only be processed according to instructions.

	implemented
Agreement of order processing with regulations on rights and obligations of contractor and client	✓
Designation of contact persons and/or responsible employees	✓
Written data protection briefing for all employees with access rights	✓
Commitment of all employees with data access rights to data confidentiality.	✓