DATA PRIVACY DIGITAL SOLUTIONS
Doka Formwork Australia Pty Ltd

I. DATA PROCESSING AGREEMENT

1. GENERAL

1.1. This Data Processing Agreement ("**DPA**") governs the rights and obligations of Doka as processor and the customer as controller in the context of processing personal data on behalf of Doka.

1.2. This DPA applies to all activities in which the processor or authorised subcontractors (sub-processors) process the customer's personal data.

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

2. OBJECT AND CONTENT OF THE PROCESSING

2.1. The processing is based on the contract concluded between the parties (Offer and Doka Terms Digital Solutions) according to which the Processor provides the Customer with certain services by means of a software application and/or a web portal and the related support services (e.g. "Professional Services such as support and maintenance, other services) (the "**Contract"**). In this context, the Processor will process personal data of Authorised Users/Users/Users (usually employees of the Customer), as well as of any other persons involved in construction projects (employees of builders, subcontractors, architects, suppliers) and other groups of persons whom the Customer names to the Processor or whose data the Processor uploads as controller, for the purpose of providing and rendering the Service.

2.2. The following data categories are processed on behalf of the controller: Name, contact data (such as e-mail address, telephone numbers, etc), contract data, login data (username and password), log data (date and time), selected operating device, company, affiliation and function in the company, location, role in the service, preferred language, vehicle registration number, logs (images), data when requesting support services (e.g. "tickets").

2.3. Data entered in the service for material management, the customer's construction projects and construction sites, measurement data, inventory data, material movement data, article master data, financial data, order data, are not covered by this DPA.

2.4. The purpose of the processing of personal data is the fulfilment of the activities that are specified as a service in the main contract or for which the customer has subsequently issued instructions to the processor.

2.5. The duration of processing is governed by the provisions of the main contract, whereby further obligations may arise from statutory provisions.

3. RIGHTS AND OBLIGATIONS OF THE PROCESSOR

3.1. The Processor shall process the Personal Data only on the basis of the Main Agreement, this DPA and the documented instructions of the Customer - including in relation to the transfer of Personal Data to a third country or an international organisation - unless the Processor is required to do so by Union or Member State law or by any other applicable law to which the Processor is subject, in which case the Processor shall notify the Customer of such legal requirements prior to processing, unless the law in question prohibits such notification on grounds of important public interest.

3.2. The processor guarantees that the persons authorised to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.

3.3. The Processor shall take all measures within its sphere of influence in accordance with Article 32 GDPR (see the Annex to this DPA). These measures are subject to technical progress and the state of the art. Minor developments shall be made without agreement with the customer.

3.4. The Customer authorises the Processor to use sub-processors (in particular IT service providers). It must be ensured that the sub-processor enters into the same obligations that are incumbent on the processor on the basis of this agreement. If the sub-processor fails to fulfil its data protection obligations, the Processor shall be liable to the Customer for compliance with the obligations of the sub-processor.

3.5. The sub-processors posted on https://www.doka.com/sub-processors in particular are covered by the general authorisation in accordance with point 3.4.

3.6. The processor undertakes to only transfer personal data outside, or to, the European Economic Area if appropriate safeguards are in place to ensure compliance with applicable data protection laws (e.g. conclusion of standard contractual clauses).

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 Processor's sole discretion – (i) an email to the Customer; or (ii) publication on the customer portal or the customer platform; or (iii) publication on https://www.doka.com/sub-processors shall be sufficient, and hereby grants the Customer the right to object to the engagement of a new or replacement of an existing sub-processor, provided that such sub-processor demonstrably fails to ensure the same or a reasonably comparable level of protection for the processing of personal data. The customer's objection shall constitute good cause for the processor to terminate the contract within the meaning of the contractual terms. An objection by the Customer that does not fulfil the aforementioned requirements shall be irrelevant.

3.8. Given the nature of the processing, the Processor shall, where possible, support the Customer with appropriate technical and organisational measures to comply with its obligation to respond to requests to exercise the rights of the data subject 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 on the basis of the information provided by the data subject. The Processor shall not be 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 anonymise or delete all personal data within a period of one hundred and eighty (180) days after completion of the provision of the processing services, unless there is an obligation to store the personal data under Union law or the law of the Member States or any other applicable law the data is required for the assertion, exercise or defence of legal claims.

3.10. Prior to anonymisation or erasure, the customer may receive the personal data in a commonly used electronic format selected by the processor against reimbursement of reasonable costs.

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 set out in Articles 32 to 36 GDPR.

3.12. The Processor shall provide the Customer with all information necessary to demonstrate compliance with the obligations set out in this DPA and shall carry out checks in accordance with point 4.5 of this DPA and contribute to them. However, the Customer agrees that inspections pursuant to Section 4.5 may, at the discretion of the Processor, be replaced by the provision of detailed documentation on the data protection and security measures implemented, relevant certifications or reports from external auditors.

3.13. The processor must inform the customer immediately if it believes that a specific instruction from the customer violates applicable data protection regulations.

4. RIGHTS AND OBLIGATIONS OF THE CUSTOMER

4.1. The Customer shall be solely responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects and for the necessary notifications to the Processor. The Customer shall inform the Processor of the contact point for all questions arising from or in connection with this DPA.

4.2. The customer shall issue all orders, partial orders or instructions that deviate from or supplement the main contract in writing. In urgent cases, instructions may be issued verbally. The customer shall confirm such instructions in writing without delay.

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

4.4. The customer shall not process any special categories of personal data without the written consent of the processor. The customer shall not process any data of persons under the age of 14 or the age restriction under any other applicable law.

4.5. Subject to Section 3.12 of this DPA, the Customer shall be entitled to inspect compliance with the obligations set out in this DPA itself or through third parties contractually or legally bound to confidentiality, provided that they are not competitors of the Processor and its affiliated companies, on site. The Customer or a third party authorised by the Customer shall comply with the Processor's internal security requirements (in particular in accordance with the applicable security and IT guidelines) as part of such checks. Due to confidentiality or security requirements, on-site controls of certain environments and information (e.g. due to jeopardising the rights of third parties or to protect business secrets) may be restricted to the extent necessary. Environments that are irrelevant to the obligations set out in this DPA are expressly excluded from the customer's right of inspection.

4.6. The customer shall bear the costs of this audit. Inspections must be carried out 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 working days), if possible over a maximum of one day according to a mutually agreed schedule that minimises 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 made in writing and must be expressly labelled as such.

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

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

Technical and Organisational Measures according to Art. 32 GDPR

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

a) Entry Control

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

	Implemented
Entry control system, card reader (magnetic/chip card)	✓
Door security (electric door opener, number lock, etc.)	✓
Security doors / windows	✓
Fence systems	✓
Key management, documentation of key allocation	✓
plant security, porter, security service	✓
Alarm system	✓
Special protection measures for the storage of backups and/or other data carriers	✓

Non-reversible destruction of data media	✓
Employee 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 persons from accessing data processing systems:

	implemented
Personal and individual user log-in when logging on to the system or company network	✓
Authorization process for access permissions	✓
Limitation of authorized users	✓
Single sign-on	✓
Password policy (specification of password parameters in terms of complexity and update interval, password history)	✓
Electronic documentation of passwords and protection of this documentation against unauthorized access	✓
Logging of access to the system	✓
Additional system log-in for certain applications	✓
Automatic locking of clients after a certain period of time without user activity (also password-protected screen saver or automatic pause)	✓
Up-to-date firewall	✓
Up-to-date antivirus software	✓

c) Access Control

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

	implemented
Central administration and documentation of authorizations	✓
Conclusion of contracts for commissioned data processing for the external maintenance of data processing systems, provided that remote maintenance involves the processing of PII, i.e., the handling of personal data, as part of the service	✓
Authorization process for permissions	✓
Authorization routines	✓
Profiles/roles	
Encryption of hard disks and/or laptops	✓
Segregation of Duties process	✓
Non-reversible deletion of data media	✓
Privacy screens for mobile data processing systems	✓
Patch management	✓

d) Separation Control

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 environment	✓
Authorization concept	✓
Network segmentation	✓

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

a) Disclosure Control

It is ensured that personal data cannot be read, copied, modified or removed 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 are implemented to ensure this:

	implemented

Encryption of the storage medium of laptops	✓
Secured file transfer (Collaboration, Sharepoint)	✓
Secured data transport (e.g., TLS)	✓
Electronic signature	✓
Secured WLAN	✓
Regulation for handling mobile storage media (e.g., laptops, USB stick, cell phone)	✓
Tunneled remote data connections (VPN = Virtual Private Network)	✓
Data classification	✓

b) Input Control

The following measures ensure that it is possible to check 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)

Availability control and resilience control

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

	implemented
Established backup procedure	✓
Storage process for backups (e.g., fire-protected safe, separate fire compartment).	✓
Ensuring data storage in the secured network	✓
Installing security updates as needed	✓
Mirroring of hard disks	✓
Installation of an uninterruptible power supply (UPS)	✓
Suitable archiving space for paper documents	✓
Fire and/or extinguishing water protection of the server room	✓
Fire and/or extinguishing water protection of the archiving rooms	✓
Air-conditioned server room	✓
Virus protection	✓
Firewall	✓
Redundant, locally separated data storage (offsite storage)	✓
Monitoring of all relevant servers	✓
Backup data center	✓
Critical components are redundant	✓

Procedures 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 intended to ensure that an organization that meets the basic requirements of data protection law is in place:

	implemented
Data protection policy (protection of PII)	✓
Establishment of a data protection committee	✓
Obligation of employees to maintain data secrecy	✓
Keeping 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 data subject rights	✓
Central documentation of all procedures and regulations for data protection with access for employees according to authorization	✓

b) Incident Response Management

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

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

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

The default settings must be considered both in the standardized default settings of systems and apps and in the setup of data processing procedures. In this phase, functions and rights are configured in concrete terms, the permissibility or impermissibility of certain inputs or input options (e.g., free texts) is defined with regard to data minimization, and decisions are made about the availability of usage functions (e.g., with regard to the scope of processing). Likewise, the type and scope of the personal reference or the anonymization (e.g., in the case of selection, export and evaluation functions, which can be specified and made available by default or freely configurable) or the availability of certain processing functions, logging, etc. are also specified.

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

d) Order control

The following measures ensure that personal data can only be processed in accordance with instructions.

	implemented
Agreement on commissioned processing with regulations on the rights and obligations of the contractor and client	✓
Designation of contact persons and/or responsible employees	✓
Written data protection briefing for all employees with access rights	✓
Obligation of all employees authorized to access data to maintain data secrecy.	✓