Wacker Neuson
Group

Agreement on the processing of personal data concerning EDI

On behalf of a controller in accordance with Article 28 (3) of the GDPR

1. Subject matter and duration of the agreement

(1) Subject matter

The subject matter results from the framework agreement on structured electronic data interchange (EDI) to which reference is made here (hereinafter referred to as the Framework Agreement).

(2) Duration

The duration of this contract (duration) corresponds to the duration of the framework agreement.

2. Scope of the agreement

(1) Mode and purpose of the proposed processing of data

For the registration of the supplier in the WebEDI portal and for the digitalization of order and delivery processing, lawfully for the execution of a contract or for contract initiation in accordance with Article 6 (1) lit b GDPR.

The performance of the data processing agreed upon shall take place exclusively in a member state of the European Union or in another member state of the Agreement on the European Economic Area. Any relocation to a third country requires prior consent of the controller and may only take place if the special requirements of Art. 44 et seq. of the GDPR are met. The appropriate level of protection is established accordingly by standard data protection clauses (Art. 46 (2) lit c, d GDPR).

(2) Data categories

The processing of personal data is subject to the following data types/categories (enumeration/description of data categories)

- Personal master data (incl. gender for purposes of communication)
- Communication data (e.g. telephone, e-mail)
- Contract master data (contractual relationship, product or contract interest)
- Billing and payment data
- Planning and control data
- IP address and log files to ensure the integrity of data transmission

(3) Categories of data subjects

The categories of data subjects to be processed shall include:

- interested individuals
- employees
- suppliers
- contacts

3. Technical and organizational measures

(1) The Processor shall document the implementation of the technical and organizational measures set out and required prior to commencement of processing, in particular with regard to the concrete execution of the contract, and shall hand them over to the Controller for review. If accepted by the Controller, the documented measures become the basis of the agreement. If the Controller's inspection/audit reveals a need for adjustment, this shall be implemented by mutual agreement.

(2) The Processor shall provide security in accordance with Art. 28 (3) lit. c, Art. 32 GDPR, in particular in conjunction with Art. 5 (1), (2) GDPR. Overall, the measures shall comprise data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. In doing so, state of the art, the implementation costs and type, scope and purpose of the processing as well as different probability of occurrence and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 (1) GDPR shall be taken into account [details in Annex 1].

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative, but adequate measures. The security level of the specified measures may not be reduced below this level. Significant changes shall be documented.

4. Correction, limitation and deletion of data

(1) The Processor may not correct, delete or restrict the processing of the data without prior written authorization from the Controller. If a data subject directly contacts the Processor in this regard, the Processor shall immediately forward this request to the Controller.
(2) As far as included in the scope of services, the deletion concept, right to be forgotten, correction, data portability and information are to be ensured directly by the processor according to documented instructions of the controller.

5. Quality assurance and other duties of the processor

In addition to compliance with the provisions of this Agreement, the Processor has legal obligations pursuant to Art. 28 to 33 GDPR; to this extent, the Processor guarantees in particular compliance with the following requirements:

a) Written appointment of a data protection officer who carries out his duties in accordance with Art. 38 and 39 GDPR, insofar as this is indicated by national supplementary laws to the GDPR. The controller must be informed immediately of any change in the data protection officer.
b) The safeguarding of confidentiality pursuant to Art. 28 (3) sentence 2 lit. b, 29, 32 (4) GDPR. In performing the processing, the Processor shall only engage employees who are obliged to maintain confidentiality and who have previously been acquainted with the data protection provisions relevant to them. The Processor and any person subordinate to the Processor who has access to personal data may only process such data in accordance with the instructions of the Controller, including the competences granted in this Agreement, unless they are legally obliged to do so.

c) The implementation of and compliance with all technical and organizational measures required for this Agreement pursuant to Art. 28 (3) sentence 2 lit. c, 32 GDPR [details in Annex 1].
d) The controller and the processor shall, upon request, cooperate with the supervisory authority in the performance of its tasks.
e) The immediate information of the controller about control actions and measures of the supervisory authority, as far as they refer to this Agreement. This shall also apply if a responsible authority investigates on the processing of personal data at the Processor's facilities as part of administrative infringement or criminal prosecution.
f) Insofar as the Controller is subject to audit by the supervisory authority, administrative infringement or criminal prosecution, the liability claim of a person concerned or a third party or any other claim in connection with the data processing at the Processor, the Processor shall support the Controller to the best of its ability.
g) The processor shall regularly monitor internal processes and technical and organizational measures to ensure that processing within its sphere of responsibility is carried out in accordance with the requirements of applicable data protection law and that the rights of the data subject are protected.
h) Proof of the technical and organizational measures taken to the controller within the scope of his supervisory duties in accordance with section 7 of this contract.

6. Sub-contracting relationships

(1) Sub-contracting relationships within the meaning of this agreement are to be understood as those services which relate directly to the provision of the main service. This does not include ancillary services which the Processor uses e.g. as telecommunications services, postal/transport services, maintenance and user services or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Processor is obliged to take appropriate contractual agreements and control measures in accordance with the law to guarantee data protection and data security of the Controller's data, even in the case of outsourced ancillary services.

(2) The Processor may commission sub-processors (other processors) only with prior written and documented consent of the Controller.

7. Supervisory duties of the Controllers

(1) The Controller shall have the right to conduct audits in consultation with the Processor. He has the right to inspect the Processor's compliance with this Agreement in its business operations by means of random checks, which are to be announced in a timely manner.
(2) The Processor shall ensure that the Controller is able to convince himself of compliance with the duties of the Processor pursuant to Art. 28 GDPR. The Processor commits to provide the Controller with the necessary information upon request and, in particular, that he will prove that the technical and organizational measures have been implemented.
(3) The processor can assert a reasonable claim for compensation to enable the controller to perform audits.

8. Notification of violations by the Processor

(1) The Processor assists the Controller in complying with the security obligations set out in Articles 32 to 36 of the GDPR, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. These include, but are not limited to

a) ensuring an adequate level of protection by technical and organizational measures which take into account the circumstances and purposes of the processing and the predicted likelihood and severity of a possible breach of rights due to vulnerabilities, and which allow the immediate identification of relevant incidents
b) the obligation to immediately report infringements of personal data to the controller
c) the obligation to assist the controller in his duty to inform the data subject and, in this context, to make all relevant information available to the controller without undue delay
d) assisting the controller in its data protection impact assessment
e) assisting the controller in prior consultations with the supervisory authority

(2) The Processor may claim compensation for support services that are not included in the Framework Agreement or are not attributable to a misconduct of the Processor.

9. Competence of the controller to issue instructions

(1) The Controller shall confirm verbal instructions without delay (at least in text form).

(2) The Processor shall immediately inform the Controller if the Processor believes that an instruction violates data protection regulations. The Processor shall be entitled to suspend the execution of such instruction until it is confirmed or amended by the Controller.

10. Deletion and return of personal data

(1) Copies or duplicates of data will not be generated without the knowledge of the Controller. Exceptions to this are backup copies, insofar as they are necessary to guarantee proper data processing, as well as data which are necessary with regard to compliance with retention obligations.

(2) After termination of the Framework Agreement, the Processor shall hand over to the Controller all data records that are connected to the controller-processor relationship and are not subject to any superordinate retention standard, or, after prior consent, destroy them in accordance with data protection regulations.

(3) Documentations which serve as proof of orderly and proper data processing shall be stored by the Processor in accordance with the respective retention periods beyond the end of the contract. He may hand them over to the Controller at the end of the contract in order to relieve him of the burden.

Wacker Neuson Group

Annex A – Technical and organizational measures

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

- Physical access control
  No unauthorized access to data centers, e.g. via magnet or chip cards, keys, electrical door openers, security service / doormen, alarm system, video surveillance;
- Logical access control
  No unauthorized usage of systems, e.g. (secure) passwords, MFA, storage encryption
- Data access control
  No unauthorized reading / writing / altering / deletion of data within systems, e.g. via access control concepts and demand-based access rights, access logging
- Separability
  Separate data processing for different purposes, e.g. multi-client processing, sandboxing;
- Pseudonymisation (Art. 32 (1) lit. a GDPR; Art. 25 (1) GDPR)
  The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures;

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

- Transmission control
  No unauthorized reading / writing / altering / deletion of data during transmission or transport; e.g. encryption in motion, Virtual Private Networks (VPN), electronic signatures;
- Input control
  Determining whether and by whom personal data have been entered, modified or removed in data processing systems, e.g.: Logging, document management;

3. Availability and resilience (Art. 32 (1) GDPR)

- Availability control
  Protection against accidental or willful destruction or loss, e.g.: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans;
- Fast recovery (Art. 32 (1) lit. c GDPR);

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

- Data Privacy Management System;
- Incident Response Management;
- Privacy by Default (Art. 25 (2) GDPR);

- Processing control
  No processing by a processor within the meaning of Art. 28 GDPR without documented instructions from the client, e.g.: Clear contract design, formalized order management, strict selection of the processor, obligation to provide prior guarantees, follow-up checks.