

Data Processing Agreement pursuant to Art. 28 General Data Protection Regulation

The new freedom in business communications.

nfon.com

1	OBJECT AND TERM OF ASSIGNMENT	5
2	ASSIGNMENT DETAILS	5
3	TECHNICAL AND ORGANISATIONAL MEASURES	6
4	CORRECTION, RESTRICTION AND DELETION OF DATA	7
5	QUALITY ASSURANCE AND OTHER PROCESSOR DUTIES	7
6	SUBPROCESSOR RELATIONS	8
7	CONTROLLER CONTROL RIGHTS	9
8	REPORTING PROCESSOR VIOLATIONS	9
9	CONTROLLER POWER TO DIRECT	10
10	DELETION AND RETURN OF PERSONAL DATA	10
11	SIGNATURES	11

Version 1.4

NFON AG
Zielstattstraße 36,
81379 München
Tel.: + 49 89 45 3000
www.nfon.com

© 2024 NFON AG - All rights reserved

Subject to change without notice
Version 1.4 / 01.2024 (EN)
effective as of 01st Jan 2024

Data Processing Agreement Pursuant to Art. 28 General Data Protection Regulation

between

- hereinafter referred to as controller –

and

NFON AG, Zielstattstraße 36, 81379 München

- hereinafter referred to as processor –



„The full provisions under Art. 28 Para. 3 General Data Protection Regulation should be included in the agreement and completed like a check list. The alternatives applicable to the specific service relationship should be ticked. Where applicable, complete blank fields per the specific assignment. Remuneration and liability provisions related to the specific processor services should be stipulated in the prime contract.”

1 Object and term of assignment

1.1 Object

The object of the contract ensues from the quotation, the current applicable Service Description, Service Level Agreement and the General Terms & Conditions.

1.2 Term

The duration of this contract (term) corresponds with the term of the applicable Service Description, Service Level Agreement and the General Terms & Conditions.

2 Assignment Details

2.1 Type and purpose of planned data processing

The type and purpose of the processor processing personal data for the controller are detailed in the applicable Service Description, Service Level Agreement and the General Terms & Conditions.

The contracted data processing shall solely be rendered in a member state of the European Union or in different signatory to the Treaty on the European Economic Area. Any outsourcing to a third country requires the prior approval of the controller and subject to the special requirements under Art. 44 ff. General Data Protection Regulation.

2.2 Type of data

The following types/categories of data (list/description of data categories are the object of processing personal data

- Key personal data
- Contract master data / account data
- Customer history
- Contract accounting and payment data
- Connection data (IP address, phone number A and B, talk time)
- Call data
- Information data (from third parties, e.g. credit agencies, or from public directories)

2.3 Categories of persons involved

The categories of persons affected by data processing include:

- Customers
- Prospects
- Employees
- Vendors
- Contacts
- Communication partners

3 Technical and Organisational Measures

- 3.1** The processor shall document the implementation of the required technical and organisational measures specified prior to awarding the contract before beginning with processing, particularly with respect to the specific job execution, and submit said to the controller for review. Upon being approved by the controller, the documented measures shall become the basis of the assignment. Any adjustments required based on a review/audit by the controller shall be mutually implemented.
- 3.2** The processor shall ensure the security required under Art. 28 Para. 3 lit. c, 32 General Data Protection Regulation, particularly in conjunction with Art. 5 Para. 1, Para. 2 General Data Protection Regulation. The measures to be taken as a whole are data security measures and measures to ensure a level of security appropriate for the risk with regard to confidentiality, integrity, accessibility, and system performance. The state of technology, implementation costs, and the type, scope and purposes of processing, along with the probability and severity of the risk to the rights and freedoms of individuals as defined by Art. 32 Para. 1 General Data Protection Regulation must be taken into account [details see appendix 1].
- 3.3** Technical and organisational measures are subject to technical progress and enhancements. In this respect the processor is permitted to implement adequate alternative measures. In doing so, the security level of the defined measures must be met. Significant modifications must be documented.
- 3.4** The processor shall provide adequate notice when changing and/or adding to technical or organisational measures. Adequate notice via the usual communication channels includes publishing a concept relatively easy for the controller to review. The processor determines the method used to provide the information. The controller shall be provided a time limit to object to these measures. The time limit is two weeks. After this time limit has expired the technical

and organisational measures are considered approved by the controller. Any objections must be submitted informally, in writing, to datenschutz@nfon.com.

4 Correction, Restriction and Deletion of Data

- 4.1** Unless required by law, the processor shall not correct, delete or limit data being processed on behalf of the controller on his own accord, but only with documented instruction from the controller. In the event a person affected contacts the processor directly in this respect, the processor shall promptly forward this request to the controller.
- 4.2** Where covered by the scope of services, the processor shall directly guarantee the principle of deletion, right to be forgotten, correction, data portability and information according to the documented instructions of the controller.

5 Quality Assurance and Other Processor Duties

In addition to complying with the provisions of this assignment, the processor shall also comply with Art. 28 to 33 General Data Protection Regulation; in this respect he shall particularly comply with the following provisions:

- Where required by law, assigning a data protection officer in writing to perform the duties under Art. 38 and 39 General Data Protection Regulation.
- The contact information for the data protection office is published on the processor's website.
- Observance of confidentiality under Art. 28 Para. 3 S. 2 lit. b, 29, 32 Para. 4 General Data Protection Regulation. The processor shall only assign employees to perform the work who are bound to confidentiality and familiar with the relevant data protection provisions. The processor and anybody working for the processor with access to personal data must only process the information as instructed by the controller, including authorisations granted by this contract unless required by law to process said.
- Implementation and compliance with all technical and organisational measures required for this assignment under Art. 28 Para. 3 S. 2 lit. c, 32 General Data Protection Regulation [details see appendix].
- The controller and the processor shall on enquiry cooperate with the regulating authority to perform their duties.
- Promptly informing the controller of audits and measures of the regulatory authority when related to this specific and general assignment unless prohibited by law. This also applies

if a competent authority is conducting an enquiry into the processor's order processing related to administrative or criminal proceedings related to the processor processing personal data by assignment.

- In the event the controller is under audit by the regulatory authority, an administrative or criminal proceedings, a liability claim by an affected person or a third party or any other claim related to the processor processing data by assignment, the processor shall support him to the best of his ability, where permitted by law.
- The processor shall regularly review internal processes and technical and organisational measures to ensure data within his area of responsibility is processed in compliance with the provisions of the relevant data protection law and to protect the rights of the affected persons.
- The technical and organisational measures taken must be documented for the controller in line with his power of audit pursuant to item 7 of this contract.

6 Subprocessor Relations

- 6.1** Within the context of these provisions, subprocessor relations are services directly related to providing the main service. This does not include additional services utilised by the processor e.g. as telecommunications services, postal/transport services, maintenance and user support or the disposal of data storage mediums and other measures to ensure confidentiality, availability, integrity and capacity of the hardware and software of data processing equipment. However, to guarantee the protection and security of the controller's data the processor is also obligated to enter into suitable contractual agreements conformable to the law with respect to additional services and implement control measures.
- 6.2** The processor is permitted to hire subprocessors (additional data processing companies) provided the controller was given appropriate notice. Suitable notice includes publishing the current and new subprocessors which the controller can review relatively easily. The information is provided via the usual communication channels. The controller shall be provided a time limit to object to these measures. The time limit is two weeks. Upon expiry of this time limit the subprocessor is deemed approved by the controller. Any objections must be submitted informally, in writing, to datenschutz@nfon.com.
- 6.3** In the event the subprocessor renders the agreed services outside the EU/EEA, the processor shall take appropriate measures to ensure admissibility under data protection laws. Such measures must also be implemented for service providers providing additional services.
- 6.4** All stipulations along the contractual chain shall also be imposed on other subprocessor. The technical and organisational measures of subprocessors must be based on the technical and organisational measures defined in this document but may be of lesser extent based on the risk.

7 Controller Control Rights

- 7.1** The controller shall be entitled to conduct audits as coordinated with the processor or, in special cases, have said conducted by an auditor to be designated. He shall be entitled to conduct spot checks at the processor's facilities, typically with due notice of at least 14 days, to verify compliance with this agreement.
- 7.2** The processor shall ensure the controller is able to verify compliance with the processor's duties pursuant to Art. 28 General Data Protection Regulation. The processor agrees to provide the controller with required information on request, and particularly to provide documentation of the technical and organisational measures being implemented.
- 7.3** Proof of such measures not only pertaining to the specific assignment may be compliance with the agreed code of conduct pursuant to Art. 40 General Data Protection Regulation:
- compliance with approved rules of conduct in accordance with Art. 40 General Data Protection Regulation
 - Certification according to an approved certification process pursuant to Art. 42 General Data Protection Regulation.
 - Actual certificates, reports or excerpts of reports from independent bodies (e.g. chartered accountant, audit, data protection officer, IT security department, data protection auditors, quality auditors).
 - Suitable certification by IT security or data protection audit (e.g. ISO27001).

The processor may request compensation for allowing the controller to conduct audits.

8 Reporting Processor Violations

The processor shall support the controller with compliance of the duties specified in articles 32 to 36 of the General Data Protection Regulation on security of personal data, reporting requirements for data breaches, data protection impact assessment and prior consultations. This include but are not limited to

- Ensuring an adequate level of security through technical and organisational measures taking into account the facts and purposes of processing along with the predicted probability and gravity of a potential infringement due to security vulnerabilities and allowing immediate detection of relevant infringements
- The duty to immediately report personal data breaches to the controller

- The duty to support the controller in his duty to report said to the affected parties and promptly provide him with all relevant information
- Supporting the controller with his data protection impact assessment
- Supporting the controller with prior consultations with the regulatory authority

9 Controller Power to Direct

- 9.1** The controllers shall promptly confirm verbal agreements in writing (text form at a minimum).
- 9.2** The processor shall promptly notify the controller if he believes an instruction violates data protection laws. The processor is authorised to suspend executing the respective instruction until confirmed or amended by the controller.

10 Deletion and Return of Personal Data

- 10.1** Data shall not be copied or duplicated without the knowledge of the controller. This does not apply to backup copies necessary to ensure proper data processing, as well as data required for compliance with statutory record retention duties.
- 10.2** Upon completing the contractual work or at the controller's request earlier – but no later than the end of the performance agreement – the processor shall return all documents obtained, the generated results of processing and use, as well as data sets related to the assignment to the controller or, with prior approval, destroy said in compliance with data protection laws. The same applies to test materials and scraps. Upon request the record of such deletion shall be presented.
- 10.3** The processor shall retain documentation for the purpose of verifying compliance with the contract and proper data processing beyond expiration of the contract in accordance with the respective retention periods. On expiration of the contract these may be transferred to the customer for purposes of relieving the processor.

11 Signatures

Place, Date

Place, Date

Signature

Signature

Name of Controller

Name of Processor

Place, Date

Place, Date

Signature

Signature

Name of Controller

Name of Processor