

Appendix 3: Data Processing Agreement Terms

Preliminary remark

This Data Processing Agreement specifies the obligations of the contracting parties with regard to data protection. It applies to all activities that are connected with the contract and in which employees of the Contractor or persons commissioned by the Contractor process personal data ("data") of the Customer or at least have access to it.

1. Subject-matter, duration, specification of the data processing

(1) The subject matter of the Agreement is the regulation of the rights and obligations of the controller (Customer) and the Contractor (Perian), insofar as personal data is processed by Perian for Customers within the meaning of the applicable data protection law as part of the provision of services (in accordance with the General Terms and Conditions and other applicable documents). The Agreement shall apply accordingly to the (remote) testing and maintenance of automated processes or data processing systems if access to personal data cannot be ruled out.

(2) The type of personal data and the categories of data subjects shall be determined and controlled by the Customer at its sole discretion.

(3) The Contractor shall not use the personal data obtained for any purposes other than the specified contractual purpose. The Contractor may anonymize the data and process and use it in anonymized form for its own purposes. The parties agree that anonymized or aggregated client data in accordance with this provision shall no longer be considered data within the meaning of this Agreement.

(4) The contractually agreed service shall be provided exclusively in a member state of the European Union, in a state party to the Agreement on the European Economic Area as well as in the UK, USA and Switzerland.

2. Customer's Right to issue instructions

(1) The Customer himself, the Customer's legal representative and the IT manager are authorized to issue instructions on behalf of the Customer. If instructions are issued by other persons, these must be confirmed by the authorized persons. The Customer shall confirm verbal instructions immediately by e-mail.

(2) The Contractor shall inform the Customer as soon as possible if it believes that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the execution of the respective instruction until it is confirmed or amended by the Customer.

(3) The Contractor shall use the data exclusively in accordance with the Customer's instructions, as conclusively expressed in the provisions of this Agreement. Individual instructions that deviate from the provisions of this Agreement or impose additional requirements shall require the Contractor's prior consent.

3. Obligations of the Customer

(1) The Customer shall be responsible for the lawfulness of the processing of the data and for safeguarding the rights of the data subjects. Should third parties assert claims against the Contractor due to the processing of data, the Customer shall indemnify the Contractor against all such claims upon first request if the Contractor proves to the Customer that it is in no way responsible for the circumstance through which the damage occurred.

(2) The Customer is the owner of the data and holder of any rights relating to the data.

(3) The Customer shall be responsible for providing the Contractor with the data in a timely manner for the provision of services under the main contract and shall be responsible for the accuracy of the data. The Customer must inform the Contractor immediately and in full if it discovers errors or irregularities with regard to data protection regulations or its instructions when checking the Contractor's contract results.

4. Quality assurance and other obligations of the Contractor

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

- a) If necessary, written appointment of a data protection officer who performs his or her duties in accordance with Art. 38 and 39 GDPR. Their current contact details will be made available on request.
- b) Maintaining confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. When carrying out the work, the Contractor shall only use employees who have been obliged to maintain confidentiality and who have previously been familiarized with the data protection provisions relevant to them. The Contractor and any person subordinate to the Contractor who has access to personal data may only process this data in accordance with the Customer's instructions, including the authorizations granted in this Agreement, unless they are legally obliged to process it.
- c) The implementation of and compliance with all technical and organizational measures required for this contract in accordance with Art. 28 para. 3 sentence 2 lit. c, 32 GDPR.
- d) The Customer and the Contractor shall cooperate with the supervisory authority in the performance of their duties upon request.
- e) Immediately informing the Customer about inspection activities and measures of the supervisory authority, insofar as they relate to this contract. This also applies if a competent authority investigates the processing of personal data in the context of administrative offense or criminal proceedings relating to the processing of personal data by the Contractor.

- f) If the Customer is subject to an inspection by the supervisory authority, administrative offense or criminal proceedings, a liability claim by a data subject or a third party or any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support the Customer to the best of its ability.
- g) The Contractor shall regularly monitor the internal processes and the technical and organizational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.
- h) Demonstrability of the technical and organizational measures taken to the Customer within the scope of the Customer's control authorizations under this Agreement.

5. Technical and organizational measures

(1) The Contractor shall document the implementation of the technical and organizational measures outlined and required prior to the awarding of the contract, particularly concerning the specific execution of the contract, before commencing processing, and shall provide this documentation to the Customer for review upon request. If the Customer's review/audit identifies a need for adjustments, these shall be implemented by mutual agreement.

(2) The Contractor shall establish security in accordance with Art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are 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 processing systems. The state of the art, the costs of implementation and the nature and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be taken into account.

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the Contractor shall be permitted to implement alternative adequate measures, provided that the security level of the specified measures is not diminished.

6. Notification of the Contractor in the event of violations

(1) The Contractor shall support the Customer in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes, inter alia

- a) ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the predicted probability and severity of a possible breach of rights through security gaps and enable the immediate detection of relevant breach events,
- b) the obligation to report personal data breaches to the Customer without delay,

- c) the obligation to support the Customer in the context of his obligation to inform the data subject and to provide him with all relevant information in this context without delay,
- d) the support of the Customer for their data protection impact assessment,
- e) supporting the Customer in the context of prior consultations with the supervisory authority.

(2) The Contractor may claim remuneration for support services that are not included in the service description or are not attributable to misconduct on the part of the Contractor.

7. Inspection rights of the Customer

(1) The Contractor shall ensure that the Customer can verify the Contractor's compliance with its obligations under Article 28 GDPR. The Customer generally has the right, in coordination with the Contractor, to conduct inspections or have inspections carried out by auditors designated on a case-by-case basis. The Customer has the right to verify the Contractor's compliance with this Agreement at the data processing site through spot checks, which must be scheduled with two weeks' notice.

(2) At the Contractor's discretion, compliance with the technical and organizational measures may be demonstrated, instead of an on-site inspection, by presenting a suitable, up-to-date attestation, reports, or excerpts of reports from independent bodies (e.g., auditors, internal audits, data protection officers, IT security departments, data protection auditors, or quality auditors) or by a suitable certification from IT security or data protection audits—e.g., in accordance with BSI-Grundschutz-("Audit Report"), provided that the Audit Report reasonably enables the Customer to verify compliance with the technical and organizational measures. If the Customer, based on actual evidence, has justified doubts that these audit reports or certifications are inadequate or incorrect, or if special incidents within the meaning of Article 33 para. 1 GDPR occur in connection with the performance of data processing on behalf of the Customer, the Customer may conduct on-site inspections.

(3) The Customer is aware that the Contractor uses the subcontractors named in Annex 2 to fulfill its contractual obligations. Therefore, only access to these systems takes place at the Contractor's place of business; the place of data processing is therefore the subcontractor's IT system. Via these systems of the subcontractor and the Contractor's access systems, the Contractor undertakes to provide the Customer with evidence of the implementation of the technical and organizational measures upon request.

(4) The Contractor is entitled, at its own discretion, taking into account the Customer's legal obligations, not to disclose information that is sensitive with regard to the Contractor's business or if the Contractor would violate legal or other contractual regulations by disclosing it. The Customer is not entitled to have access to data or information about other customers of the Contractor, to information relating to costs - unless these form the basis of reimbursable or pass-through

expenses - to quality review and contract management reports and to any other confidential data of the Contractor that is not directly relevant to the agreed inspection purposes.

(5) The Customer shall inform the Contractor in a timely manner (at least two weeks in advance) of all circumstances related to the execution of the inspection. As a rule, the Customer may carry out one inspection per calendar year. This shall not affect the Customer's right to carry out further inspections in the event of special incidents.

(6) The Contractor shall receive compensation for expenses from the Customer if the manner of an inspection disproportionately affects the Contractor.

(7) If the Customer commissions a third party to carry out the inspection, the Customer shall obligate the third party in writing in the same way as the Customer is obligated to the Contractor under this Agreement. In addition, the Customer shall bind the third party to secrecy and confidentiality, unless the third party is subject to a professional confidentiality obligation. At the Contractor's request, the Customer shall immediately submit the obligation agreements with the third party to the Contractor. The Customer may not commission a competitor of the Contractor with the inspection.

8. Subcontracting relationships

(1) Subcontracting relationships within the meaning of this provision shall be understood as those services that relate directly to the provision of the main service. This does not include ancillary services which the Contractor uses, e.g. as telecommunications services, postal/transport services, maintenance and user service 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 Contractor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure the data protection and data security of the Customer's data, even in the case of outsourced ancillary services.

(2) The Contractor may only commission subcontractors (other processors) with prior specific written authorization of the Customer. The Customer agrees to the commissioning of the subcontractors named in the Annex on the condition of a contractual agreement in accordance with Art. 28 (2-4) GDPR.

(3) The replacement of an existing subcontractor is permissible insofar as:

- the Contractor notifies the Customer of such outsourcing to subcontractors a reasonable time in advance in writing or in text form and
- the Customer does not object to the planned outsourcing in writing or in text form to the Contractor by the time the data is handed over and
- a contractual agreement in accordance with Art. 28 (4) GDPR is used as a basis.

(4) The transfer of the Customer's personal data to the subcontractor and the subcontractor's initial engagement are only permitted once all requirements for subcontracting have been met. The obligations under data protection law arising from this Agreement shall be transferred to the further processor.

9. Rights of the data subjects

(1) The rights of the persons affected by the data processing must be asserted against the Customer.

(2) If a data subject directly contacts the Contractor regarding access, rectification, erasure, or restriction of their personal data, the Contractor shall promptly forward this request to the Customer.

(3) If a data subject exercises their rights to rectification, erasure, or restriction of data, or to access information regarding stored data, the purpose of the storage, and the persons and locations to which the data is regularly transferred, the Contractor shall assist the Customer in fulfilling these claims to the extent reasonable and necessary for the Customer, provided the Customer cannot fulfill the claims without the Contractor's assistance. The Contractor shall receive reasonable compensation from the Customer for the effort incurred in the course of such assistance.

(4) The Contractor shall enable the Customer to rectify, erase, or restrict data, or, upon the Customer's request, carry out the rectification, restriction, or erasure themselves if and to the extent that it is impossible for the Customer to do so.

10. Rectification, restriction and erasure of data

(1) The Contractor may not rectify, erase or restrict the processing of data processed on behalf of the Customer without authorization, but only in accordance with documented instructions from the Customer. If a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Customer without delay.

(2) Any deletion concept, the guarantee of the right to be forgotten, correction, data portability and information must be ensured directly by the Customer.

11. Deletion and return of personal data

After completion of the provision of the processing services, the Contractor shall, at the Customer's discretion, either delete all personal data or return it to the Customer, unless there is an obligation to store the personal data under Union or German law or unless otherwise stated in the service descriptions and the respective contractual agreements.

12. Relationship to the main contract

Insofar as no special provisions are contained in this Agreement, the provisions of the main contract shall apply. In the event of contradictions between this Agreement and provisions from other

agreements, in particular from the main contract, the provisions from this Agreement shall take precedence.

13 Termination of previous agreements

The parties agree that any existing agreements on data processing between the parties shall be mutually terminated and replaced by this new Data Processing Agreement concurrently with the commencement of this Agreement.

14. References to the GDPR

All references to the GDPR contained in this Agreement apply to the GDPR in its current version or any successor regulations.

Status September 2024