Agreement on the Processing of Personal Data

on behalf of a Controller implementing Regulation (EU) 2016/679
(General Data Protection Regulation/GDPR)

concluded by and between

(hereinafter referred to as the “Customer”)

APA-IT Informationstechnologie GmbH
Laimgrubengasse 10, 1060 Vienna
(hereinafter referred to as the “Contractor”)

PREAMBLE

To ensure compliance with the mandatory provisions of Regulation (EU) 2016/679 (General Data Protection Regulation/GDPR) the parties agree that all contractual arrangements on data protection matters in existing contracts will be replaced by the present Agreement with effect as of 25 May 2018, unless the present Agreement provides otherwise. The validity of the remaining provisions shall remain unaffected. In the case of contradictions the provisions of the present Agreement shall prevail.

SCOPE OF THE PROCESSING ACTIVITIES

1. The duration of processing shall depend on the underlying civil-law transaction which the Contractor carries out on behalf of the controller. The purpose of processing, the categories of data subjects and the types of personal data shall depend on the relevant product and can be found at https://apa.at/about/auftragsverarbeitung/.

II. DATA PROTECTION

1. The parties undertake to comply with the regulations of Austrian and European data protection law applicable from time to time. The Contractor shall use all data exclusively for the purposes of performance of the Agreement on behalf of the Customer.
2. The Contractor undertakes to process personal data only upon a documented instruction from the Customer, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the Contractor is subject; in such a case, the Contractor shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
3. The Contractor shall process personal data exclusively upon documented instruction. If data subjects contact the Contractor directly, the Contractor shall immediately forward that request to the Customer. The Contractor shall inform the Customer pursuant to Art. 28 (3) (h) GDPR if, in his opinion, an instruction infringes upon the GDPR or other applicable data protection provisions.
4. The parties put on record and agree that the Contractor possesses sufficient expertise, reliability and resources and will take appropriate technical and organisational measures in such a manner that the requirements of the GDPR will be fulfilled.
5. The Contractor ensures that persons authorised to process the personal data have committed themselves to confidentiality. The obligation of confidentiality of the persons in charge of data processing shall continue to apply even after they stop working for and leave the Contractor.
6. The Contractor can use sub-processors. Agreed sub-processors commissioned at the time of conclusion of this contract are available in the product sheet (https://apa.at/about/auftragsverarbeitung/) and are approved by the Customer. For further sub-processors: The Contractor will inform the Customer of the following planned changes: name and address of the sub-processor, description of the planned change. The Contractor concludes the required contract within the meaning of Article 28 Paragraph 4 GDPR with the sub-processor. It must be ensured that the sub-processor assumes the same obligations that the Contractor has on the basis of this contract. Sub-processors in third countries may only be commissioned if the special requirements of Article 44 ff of the GDPR are met. The Contractor must inform the Customer of the intended involvement of other sub-processors in writing (e.g. by email) in good time (at least 14 days in advance) so that he can, if necessary, raise an objection in writing. If the Customer does not raise a written objection within 7 days, the change is deemed approved. An objection may only be made for important reasons and with appropriate justified justification (e.g. previous data protection violation by the sub-processor). If the Customer raises such an objection, although the Contractor continues to contractually ensure compliance with the rights and obligations under this ADV, the Contractor is entitled to extraordinary termination of the entire contractual relationship without notice. If the Customer raises such an objection, the Contractor can subsequently announce that it will not use this sub-processor or at least not with services relevant to data protection law. If the Contractor cannot confirm this, the Customer is entitled to terminate the entire contractual relationship extraordinarily and without notice. For example, general auxiliary services from third parties in the areas of telecommunications, shipping/transport or IT support are not considered to be relevant sub-contractual relationships in this sense, although risk-appropriate and legally compliant contractual regulations or control measures must always be ensured.
7. The Contractor undertakes to assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer‘s gainful obligation to respond to requests for exercising the data subject‘s rights. In particular, the Contractor shall forward enquiries, complaints and requests he receives from data subjects to the controller.

8. The Contractor shall make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in this Agreement. The Contractor shall, subject to appropriately early written notice, allow the Customer and/or an auditor mandated by the Customer to carry out audits or inspections of the Contractor's systems and processes with regard to the personal data that is processed on behalf of the Customer, provided that such audits or inspections are carried out during the Contractor's normal business hours and with minimum disturbance of his operations and that the Customer will treat as strictly confidential all information gained in this connection, unless the Customer is obliged to disclose such information by law. All costs incurred by the Contractor in connection with the provision of such information, approval of such audits or inspections and otherwise in connection with this clause shall be borne by the Customer.
9. The Contractor undertakes to either delete or return, at the choice of the Customer, all personal data after the end of the provision of services relating to processing, unless Union or Member State law requires storage of the personal data.

III. DATA SECURITY

1. Existing arrangements regarding the data security measures to be taken by the Contractor shall remain unaffected by this provision and shall continue to apply without changes. Liability limits expressed in figures, if any, shall depend on the basic contract underlying this Agreement.
2. Unless at the date of this Agreement arrangements were made regarding the security measures to be taken, the data security measures described in Annex 1 shall be deemed sufficient. Apart from that, further measures may be agreed for specific data processing activities.
3. The Contractor shall adapt the measures stated in Annex 1 to the state of the art, where necessary, and inform the Customer thereof.
4. The Contractor shall support the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR on the security of personal data, taking into account the nature of processing and the information available to the Contractor.
5. Gainful services: all services to be rendered by the Contractor shall, in principle, be gainful. Unless regulated otherwise in the basic contract, services shall be billed as incurred according to the currently applicable hourly rates of APA-IT.

ANNEX

APA-IT is the competent partner for implementation and operation of IT products. Alongside the implementation and operation of IT products, data protection and information security have always been at the centre of our activities. APA-IT has obtained comprehensive certification for the processes that serve the purpose of operation of IT products.

In the field of information security the ISO/IEC 27001:2013 standard has become established. The ISO/IEC 27001:2013 standard imposes requirements for an information security management system (ISMS) that serves the purpose of taking into account information security in processes that also serve the purpose of implementing customer requirements. The managing bodies of APA-IT have put themselves and their staff under an obligation to comply with the ISO/ IEC 27001:2013 standard by publishing internal policies. Regular trainings regarding the contents of the standard are held, which are checked for their effectiveness in the course of audits that are carried out both by external accredited institutes and by APA-IT staff. The ISO/IEC 27001:2013 standard is state of the art in the field of information security.

By introducing the ISMS APA-IT also fulfils the obligations regarding data security laid down in Regulation (EU) 2016/679 (General Data Protection Regulation/GDPR). In terms of data protection law the following technical and organisational measures are of particular importance as they may be understood as a specification of the abstract term of technical and organisational measures of the GDPR. Such measures include but are not limited to physical access control, electronic access control, internal access control, data transfer control, transport control, data entry check, order control, availability check and data storage media control.

The measures in detail

APA-IT carries out **physical access control** by having put the server rooms in a separate area. Access is secured by an access control system. A CCTV system is in place. Only authorised persons are granted access. APA-IT carries out **internal access control** by means of an authorisation system. Only named users are being used. Access authorisations are checked for their appropriateness once a year. Access authorisations depend on the processing agreements. APA-IT fulfils its **documentation duty** and carries out **data entry checks** by keeping a secure log or by documentation in the event log. Those log files serve the purpose of identifying unlawful use of data and defence against attacks. The logs will be checked by the Chief Information Security Officer (CISO) in accordance with the audit plan. APA-IT carries out **data transfer control and transport control** by classifying information, on the one hand, and by encrypting mobile devices, on the other hand. Communication is effected via encrypted channels. APA-IT fulfils the requirement that use of data must be bound to orders by granting users access only to systems to be used for performance of the contract. IT policies regulate handling of such systems. APA-IT carries out the availability check by means of redundant management of the computing centre. The systems are secured in accordance with the requirements of a backup concept. The backups are checked for their correctness. APA-IT staff are put under a comprehensive obligation to maintain data secrecy. This obligation shall be fulfilled even after termination of the employment relationship.

Confirmation of effectiveness

TÜV AUSTRIA Deutschland GmbH (TÜV) has certified APA-IT's ISMS. TÜV itself is an independent certification agency accredited by the government. The certificates may be retrieved from the link stated in Clause 1.