APLEONA

Released for public use

Supplementary Contractual Conditions of the Apleona Group on Information Security Requirements for Suppliers

Table of contents

1 Preamble

- The contractor shall support the client by providing services supported by information technology (e.g. consulting activities), or shall supply or make available to the client IT (Information Technology) or OT (Operational Technology) products, which shall be specified in more detail in the Contract.
- These contractual conditions regulate supplementary information security requirements to be fulfilled by the contractor.
- The information and applications covered by the contract are subject to a defined protection requirement (normal, high, very high), from which the concrete design of the information security measures is derived. The protection requirement itself, as well as details of measures, are described in the service description or in the contract.
- In addition to these Supplementary Terms and Conditions of Apleona GmbH on Information Security Requirements, information security requirements of a client may be passed on to the contractor in individual cases. These are part of the contract between the client and the contractor. With regard to the order of priority of information security requirements of different origin, the following applies: First the requirements of the client's customers, then these Supplementary Terms and Conditions of Apleona GmbH on Information Security Requirements.
- Unless expressly agreed otherwise, any expenses incurred by the contractor due to the implementation of the following requirements shall be compensated with the agreed remuneration.

2 Information security requirements

2.1 Information security management

The contractor has established suitable processes in its company to ensure information security within the scope of the provision of services and shall maintain this throughout the entire term of the contract. This is done, for example, in the form of an appropriate information security management system (ISMS) or through equivalent, suitable processes for ensuring information security within the scope of the provision of services. The contractor's information security processes comply at least with the information security requirements described below and are based on ISO/IEC 27001 or an equivalent requirement.

2.2 Roles and contact persons

a) Information Security Coordinator

The contractor must appoint a competent contact person (e.g. Information Security Officer, IT Security Manager or Chief Information Security Officer (CISO)) for all aspects of information security, who is able and authorised to provide information to the client on all questions of information security management.

b) Contact person for regular communication

The client may require the contractor to name further contact persons / persons responsible for roles in all information security-related matters in the context of the commissioned service (e.g. professional, technical or operational persons responsible) and to clarify the distribution of tasks and the transfer of responsibility beyond doubt. The contractor shall notify the client of any changes without delay.

c) Emergency coordination contact

The contractor shall appoint a central contact person (Single Point of Contact (SPOC)) for emergency communication who is available to the client. In the event of an emergency, the SPOC has access to all necessary data of the contractor (e.g. product monitoring, identity access management (IAM) and configuration data) and makes these available to the client and its emergency team on request and in a suitable format (readable and processable).

2.3 Security check

The client reserves the right to require the contractor to carry out a security check in accordance with the *Handbook for Secret Protection in the Economy* of the German Federal Ministry for Economic Affairs and Energy ("*Secret Protection Handbook*") for employees or other persons deployed by the contractor within the scope of the provision of services who come into contact with information and systems categorised by the client as requiring special protection or critical infrastructures within the meaning of the Ordinance on the Determination of the German Critical Infrastructures under the BSI Act (BSI-KritisV). The contractor shall provide the client with proof of the successful performance of the security check in text form.

2.4 Status report

The client may request a status report from the contractor on the information security of the purchased service. This contains, for example, information on deviations from agreed information security requirements, progress statistics on security incidents and security patches, status on vulnerability management and audit results, availability of security controls, efforts to rectify incidents and invoicing in the case of separate agreements on security measures.

2.5 Qualified staff

The contractor shall ensure that the personnel it employs have the necessary qualifications and awareness with regard to the requirements for information security for the performance of the order and shall prove this to the client upon request.

2.6 Subcontractor obligation

The contractor warrants that its subcontractors used in relation to this contractual relationship and, to the extent agreed in the contract, their subcontractors comply with the requirements of this contract, those of ISO/IEC 27001 or those of a comparable standard. It shall provide corresponding evidence at the request of the client.

2.7 Encryption

The contractor shall guarantee encrypted transmission and storage of data of the levels "confidential" and "strictly confidential". If the data is not stored at the contractor's premises, the client shall be notified accordingly.

2.8 Legal Spaces Hosting

The contractor undertakes to name all countries in which data of the client are processed or stored or applications are operated by the contractor or one of its subcontractors. The contractor hereby assures that the data will not leave the named storage locations. Movements within the EU are excluded from this, but must be notified to the client in text form without delay. A breach of this provision entitles the client to terminate the contract without notice.

2.9 Data deletion

The Contractor warrants to immediately and securely delete and destroy all data related to the contractual relationship at all primary and secondary locations of the contractor and its subcontractors upon termination of the contract so that it cannot be restored. Exceptions exist only in the case of data which the Contractor is legally obliged to retain or for which this has been contractually agreed. The contractor shall provide evidence of this at the client's request.

2.10 Terminals

If the contractor uses its own end devices to provide the agreed service, it undertakes to comply with the client's specifications set out below. For the purposes of this provision, end device means any IT asset of the contractor that is connected to IT applications and IT infrastructure of the client (wired or wireless) or that is used to process data of the client.

- The end devices must be secured according to the current state of the art.
- Privileged (e.g. administrative) accounts are separate from standard accounts and may not be used for daily work.
- The contractor undertakes to report the compromise of a terminal device immediately to the client's responsible persons and to deactivate and block it without delay.
- The use of hacking tools and similar applications is prohibited unless expressly permitted.
- The contractor shall be responsible for ensuring that there is no network coupling of the client's data networks and the companies affiliated with the client with other data networks.

2.11 Security incident reporting

The contractor undertakes to inform the client of all security incidents or data protection breaches pursuant to Art. 33 of the GDPR that occur in the environment of the contractor or one of its subcontractors and have an impact on its direct or indirect provision of services. The notification must be made immediately if the security incident is relevant to the data and systems of the Principal and its affiliated companies. Security incidents that do not affect the client's data and systems shall be disclosed to the client as part of the status report.

2.12 Restore safe condition

In the event of a security incident relevant to the client and its affiliated companies, the contractor shall, in addition to informing the client, also immediately take all necessary measures to restore the required security. If concerted action with the client is required for this purpose, the contractor shall contact the client with a detailed catalogue of measures and coordinate with the client. If the support of third parties is necessary for the processing of the measures, the contractor shall grant them access to all necessary information, systems and operating sites.

2.13 Access

The contractor shall only be permitted direct or covert access to the information systems (e.g. infrastructure, programmes, databases) of the client and its affiliated companies if it has received express, documented access authorisation from the client. The access authorisation is limited to the deployed and expressly authorised employees of the contractor or its subcontractors. The transfer of access authorisation to third parties is prohibited. Any access authorisation granted may only be used within the scope of the services assumed under the contract.

2.14 Operational security

The client reserves the right to carry out blocking and monitoring on the basis of official orders or the terms of use. Likewise, an interruption of the network access is possible at any time if the operational security, the operational behaviour, the network or other devices or software connected to it are impaired in any way by the devices of the contractor connected to the network. The above shall apply subject to deviating regulations on the handling of personal data in the contractual relationship.

3 Assessment of the contractor's information security maturity level

3.1 Information from the security organisation

The contractor shall disclose information on its security organisation to the Client upon request, on the basis of which the client can carry out an assessment of the maturity level of information security. This may be, for example, a management summary on the security organisation in the scope of the service, reports from an existing information

security management system, an ISO/IEC 27001 certificate, including the statement of applicability or equivalent evidence or current audit results in the scope of the service.

3.2 Audit

The contractor agrees that the client or a third party commissioned by the client may audit the contractor during the term of the contract with regard to its information security and compliance with data protection provisions.

The basis of the information security audits is ISO/IEC 27001 and the current state of the art. The audits examine the appropriate implementation of the agreed information security requirements in relation to the contract (service, product) and the structure and effectiveness of the contractor's information security organisation. The basis of the data protection audits is the DSGVO and the BDSG.

As a matter of principle, audits should be carried out at least two years apart. They shall be carried out during normal business hours and the duration of the on-site audit part shall be limited to one to two working days if possible. The client shall announce an occasion-free regular audit at least six weeks before it is carried out. Occasion-related audits can also be carried out at shorter notice depending on the severity of the occasion or the urgency.

The contractor shall provide the required documents such as management reports, operational documents (configuration and authorisation data), reports from the ISMS in good time (usually no later than three weeks before the date of the audit) and shall fulfil its duties to cooperate, e.g. granting the necessary access rights, providing documentation and access, within the scope of the audit.

The client shall provide the contractor with the results of the audit in report form. The contractor undertakes to rectify the deviations identified as critical and to report on the progress of the rectifications. The client and the contractor shall mutually agree on the scope and schedule of these improvement projects. The client reserves the right to check the progress of the improvement measures on site. The period mentioned above for regular audits shall apply to the preparation of these audits. The costs incurred by the client for an ad hoc regular audit shall be borne by the client. The costs incurred by the client for an occasion-related audit, e.g. initiated by a security incident, shall be borne by the contractor.

Insofar as an audit can demonstrably not be carried out as planned by the client for reasons of professional law, the contractor shall inform the client of these reasons in a timely manner. The parties shall then agree on a modified audit plan. In doing so, both the professional law applicable to the contractor and the interests of the client are taken into account.