Information Security and Data Protection: Obligations of External IT Service Providers

Section one - General Terms and Conditions

1. Introduction

The JUWI Group has set out its strategy with regard to the protection of corporate information in a superordinate “Guideline on Information Security”. This is intended to ensure compliance with the internal stipulations regarding information security and statutory regulations.

For this reason, the Information Security Officer (ISB) has formulated requirements and stipulations for cooperation with IT service providers (hereinafter referred to as “**contractors**”) in this document “**Information Security and Data Protection: Obligations for External IT Service Providers**”. It applies to all types of IT services for all companies within the JUWI Group (hereinafter referred to as the “**client**”).

2. Security Guideline

(1) These obligations are binding for physical and logical access to IT systems, services, information, data, and applications in networks of the JUWI Group (hereinafter referred to as “JUWI network”). It also applies for access to buildings and rooms with IT or technical components.

(2) In individual cases, it can be augmented with additional assignment-related or system-related security obligations.

(3) The Contractor must ensure the observance of these obligations within his company and among his subcontractors.

3. Access to buildings and premises

Access to the premises/offices of the JUWI Group must always be requested through a JUWI contact partner. In cases in which the contractor is issued with an access card, this must be displayed at all times. The contractor and/or his staff are, therefore, prohibited from moving around the premises of the JUWI Group unaccompanied.

Section two – Technical Security Guideline

4. Physical access and logical access rights

(1) Physical and logical access rights for the JUWI network are to be allocated according to necessity and restricted on demand. The arrangement of physical access and logical access rights for the JUWI network shall ensue through JUWI IT Support which can be contacted by email under it-support@juwi.de or by telephone under +49 6732 9657-1111 and must be applied for by the client on behalf of the contractor.

Energie-Allee 1 • 55286 Wörrstadt • Germany • Tel. +49 (0)6732 96 57-0 • Fax. +49 (0)6732 96 57-7001 • info@juwi.de • www.juwi.com

(2) Prior to the setting up of physical access/logical access, the contractor must inform his staff and subcontractors' staff about the remote access application and about this document "**Information Security and Data Protection: Obligations for External IT Service Providers**".

(3) When physical access/logical access to the JUWI network has been set up for a contractor or his subcontractors, the following rules are to be observed:

- Each employee of the contractor must register using the user ID issued to him by JUWI. The client draws the contractor's attention to the fact that physical and logical access to the JUWI network is logged and may be analyzed. The contractor must inform his staff and subcontractors of same. User IDs and passwords may not be passed on to others.
- The contractor is obliged to inform the client without delay when physical/logical access to the JUWI network is no longer required (e.g. completion of the contract, employee turnover, serving of notice or other terminaton of the contract). Physical /logical access for external staff must be limited to the planned duration of the contract, at most to a period of six (6) months.

5. Administration privileges

(1) Where the contractor requires administration privileges in order to execute the contract, this can be set up upon application of the contractor.

(2) The setting up, alteration and deletion of administration privileges for systems within the JUWI network shall ensue through JUWI IT Support.

(3) Administrators plan, install, configure and update the IT infrastructure. Within the framework of their administrative duties and privileges, they ensure:

- correct installation,
- trouble-free operation,
- appropriate updating of the IT systems and applications and
- observance of the objectives of information security (confidentiality, integrity, availability) in their area of responsibility.

(4) The contractor or his staff and subcontractors who have been issued with administration privileges must observe the following rules:

- The administration privileges granted for the execution of the contract may be used exclusively for the intended purpose. Any passing on and/or transfer of the administration privileges personally assigned for execution of the contract and related user IDs and passwords is prohibited.
- If, for technical or organizational reasons, authorizations are set up that go beyond those necessary to fulfill the contract, only authorizations that are absolutely necessary to fulfill the assignment may be used.
- Unauthorized physical and logical access to the client's IT system, services, data and applications and access outside of the contract are prohibited.
- The overriding of security measures and encoders is prohibited.
- In the execution of administrative duties, close attention must be paid to strictly ensure the confidentiality, availability and integrity of the JUWI IT systems, services, data and applications.
- Where, due to personnel-related, organizational or technical measures or changes, the requirements for the granting of administration privileges are no longer being met, either partially

Energie-Allee 1 • 55286 Wörrstadt • Germany • Tel. +49 (0)6732 96 57-0 • Fax. +49 (0)6732 96 57-7001 • info@juwi.de • www.juwi.com

or in full, or where administration privileges are no longer required, the contractor must notify the client immediately.

6. Protection of the movement of information

The following protective measures must be observed in order to protect information and the JUWI network if information is transferred and/ or processed and, where applicable, exchanged with the client and/or companies of the JUWI Group (outside of or within the JUWI network) to carry out the assignment:

- The contractor must ensure that the latest version of a recognized secure anti-virus system with a regularly updated virus signature databank is installed on hardware (e.g. PCs, servers, gateways) used and provided by him, which offers protection against malware attacks (e.g. viruses, worms, trojan horses) in particular via email, web, mobile data carriers (e.g. USB flash drives) or other media by controlling the data access.
- Where confidential information is exchanged between the JUWI network and the network of the contractor or subcontractors, the information is to be protected to a state-of-the-art standard and/or the transfer/transport must ensue via a secure connection/means of transport. For the exchange of strictly confidential information, content encryption (container, hardware encryption) and protected transmission/transport are mandatory.
- The contractor and his subcontractors must ensure by means of a defined process that correctly licensed software and regularly updated security patches for the operating system software and applications are installed on the hardware used.

7. Connection to IT systems

In the case of a connection between IT systems of the contractor's network and the JUWI network, the following rules are to be observed:

- When a connection is established to the JUWI network, the contractor and his subcontractors must ensue that their own network does not facilitate uncontrolled logical access by third parties to the JUWI network.
- The client assumes no responsibility for any damage to adjascent systems of the contractor or his subcontractors which may occur while the contractor or his subcontractors are connected to the JUWI network.

8. Use of wireless components

The use of wireless components belonging to the contractor or his subcontractors in premises of the JUWI Group may not negatively impact the existing equipment and no connection to the JUWI network may be established.

9. Secure system and applications operation

If IT systems, applications and IT infrastructure are operated or administered by the contractor in premises of the JUWI Group or the contractor on the instructions of the client (application service provider), the following rules apply:

(1) The operation must comply with the information protection stipulations in order to be recognized as trustworthy. In particular:

- the statutory stipulations must be observed,

Energie-Allee 1 • 55286 Wörrstadt • Germany • Tel. +49 (0)6732 96 57-0 • Fax. +49 (0)6732 96 57-7001 • info@juwi.de • www.juwi.com

- the general BSI standards and/or ISO 27001 must be observed,
- the best technology with regard to secure collection, processing, dissemination, storage and safekeeping, transmissions and deletion/disposal of information requiring protection and
- the requirements in terms of communication and escalation processes with regard to the events of information protection relevance are to be observed.

(2) The contractor and his subcontractors must take appropriate precautionary measures to protect the hardware components from physical damage and prevent use by unauthorized users.

(3) The contractor and his subcontractors must guarantee the security of the operating environment and implement physical and logical access controls.

(4) Where the contract involves the collection, use or processing of personal data within the meaning of the General Data Protection Regulation and the German Federal Data Protection Act, the contractor must take all the measures dictated by statutory stipulations to protect the data.

10. Software development and integration

Where the contractor renders software development and/or integration services, the project specific security requirements agreed separately between client and contractor are to be implemented, taking this document into account.

Section three – General Obligations

11. Use of client information

(1) The contractor and his subcontractors are obliged to use the physical/logical access rights (IT system, services data and applications) granted by the client exclusively in the context of the duties to be performed under the contract.

(2) All information not already in the public domain acquired through the contract, as well as copies, records and work results compiled in connection with the contract, are the property of the client and are to be returned to same upon termination of the contract.

(3) The contractor and his subcontractors are obliged to treat all information on the client and companies of the JUWI Group, their business and operating matters and all work results which come to their notice in the context of the execution of the contract confidentially and prevent their being disclosed to unauthorized persons as well as non-contractual use, reproduction or transmission. These obligations shall continue to apply beyond the termination of the contractual relationship.

(4) The contractor and his subcontractors are not permitted to acquire business or operating information of any kind regarding the client and/or his customer, supplier or staff which has not been made public by the JUWI Group or to use or copy same for their own purposes or to make copies or records of any kind which are not necessary for the execution of the contract. Information, copies, records or work results of this kind may not be passed on to third parties or disclosed to third parties.

(5) Confidential information may only be passed on to those subcontractors who have been approved by the client and bound to observance of the above document "**Information Security and Data Protection: Obligations of External IT Service Providers**".

Energie-Allee 1 • 55286 Wörrstadt • Germany • Tel. +49 (0)6732 96 57-0 • Fax. +49 (0)6732 96 57-7001 • info@juwi.de • www.juwi.com

12. Data protection

(1) The contractor guarantees that he complies with all valid data protection legislation, specifically the EU General Data Protection Regulations and the 2018 German Federal Data Protection Act and that he has obtained all the permits relating to the handling and management of personal data necessary under current legislation. The contractor shall indemnify the client from all costs, claims, liabilities and demands arising for the client with regard to an infringement of this guarantee.

(2) With the awarding of the contract, the contractor is informed that the client's **"Information on data processing for customers, suppliers and other data subjects"** is to be observed. For the event that the data subject is not also the contractor, the contractor hereby undertakes to pass this "Information on data processing for customers, suppliers and other data subjects" on to the data subjects who, on the intitiative of the contractor, will have contact with the client in the context of this contractual relationship on the intitiative of the contractor.

(3) Where, in the context of this contractual relationship, the contractor is acting as a processor within the meaning of Art. 28 GDPR, the contractor and client will first conclude a processing agreement in compliance with the statutory stipulations. The contractor and client are jointly and severally liable for compensation regarding losses suffered by any person due to inadmissable or incorrect data processing in the context of the contractual relationship. The contractor is responsible for proving that the damage did not occur as a result of a circumstance for which he is responsible, provided that the relevant data was compiled under this agreement. Until such time as this proof has been presented, the contractor shall indemnify the client, at first request, from all claims, demands, liability of third parties or vis-a-vis third parties and for costs charged against the client in the context of the processing. The contractor shall be liable to the client for damage culpably caused by the contractor, his employees or any subcontractors he may deploy in the execution of the contract. This Item 12 shall not apply provided the damage results from the correct implementation of commissioned services or actions carried out on the instructions of the client.

(4) The contractor undertakes to only design employees that have been bound to data secrecy pursuant to Section 5 BDSG (old) or to the observance of confidentiality within the meaning of the GDPR and where this obligation continues to apply for the period following termination of their employment with the contractor.

(5) Regardless of the statutory stipulations, any passing on of the client's personal data to third parties (including subcontractors) by the contractor requires the prior written approval of the client. The contractor undertakes only to commission subcontractors with the processing of the client's personal data when these have previously been bound in writing to the observance of the obligations pursuant to the above Item 12 "Data Protection" in the same manner as the contractor.

13. Personal suitability and professional qualifications of the employee

(1) The contractor is obliged to only assign empoyees to the clients who are personally suitable and professionally qualified. The contractor is to assess the employee prior to the beginning of the employment.

(2) At the request of the client, the contractor shall supply the client with suitable documents for the assessment of the personal and professional suitability of the respective employee deployed.

(3) Points 1 and 2 shall apply accordingly for employees of subcontractors of the contractor.

Energie-Allee 1 • 55286 Wörrstadt • Germany • Tel. +49 (0)6732 96 57-0 • Fax. +49 (0)6732 96 57-7001 • info@juwi.de • www.juwi.com

Section four – Monitoring of the observance of the security guideline, notification requirements and blocking of physical and logical access

14. Monitoring, notification requirement and blocking of logical access

(1) The client shall also have the right to monitor the observance of this Security Guideline at the contractor's site.

(2) The contractor shall permit access to the client, in particular following prior notification and within normal business hours, to all relevant operating sites and shall support him in all necessary activities and tests. Furthermore, he shall permit inspection of the documentation of operational relevance for the JUWI network.

(3) Furthermore, the client reserves the right to modify the type of physical/logical access to the JUWI network granted to the contractor in order to guarantee the security of the JUWI network.

(4) The contractor is obliged to comply with the security regulations and laws relevant for him, and to ensure tamper-proof documentation of all relevant errors, irregularities or security incidents as well as initiated measures to eliminate same in the context of the JUWI network, and report same immediately to the client.

Energie-Allee 1 • 55286 Wörrstadt • Germany • Tel. +49 (0)6732 96 57-0 • Fax. +49 (0)6732 96 57-7001 • info@juwi.de • www.juwi.com