Informationssicherheit und Datenschutz: Verpflichtungen für IT Fremddienstleister

Erster Abschnitt – Allgemeine Bestimmungen

1. Einleitung

Die JUWI-Gruppe hat ihre Strategie in Bezug auf den Schutz von Unternehmensinformationen in einer übergeordneten „Leitlinie Informationssicherheit“ festgelegt. Diese soll die Erfüllung der unternehmensinternen Vorgaben an Informationssicherheit und der gesetzlichen Vorschriften sicherstellen.

Aus diesem Grund hat die Informationssicherheitsbeauftragte (ISB) der JUWI GmbH, Anforderungen an und Vorgaben für die Zusammenarbeit mit IT-Dienstleistern (nachfolgend „**Auftragnehmern**“ genannt) in diesem Dokument „**Informationssicherheit und Datenschutz: Verpflichtungen für IT-Fremddienstleister**“ beschrieben. Es gilt für IT-Leistungen aller Art und für alle Gesellschaften der JUWI-Gruppe (nachfolgend „**Auftraggeber**“ genannt).

2. Sicherheitsrichtlinie

(1) Diese Verpflichtungen sind für den Zugang und Zugriff auf IT-Systeme, Dienste, Informationen, Daten und Anwendungen in Netzwerken der JUWI-Gruppe (nachfolgend „JUWI Netzwerk“ genannt) verbindlich. Sie gelten auch für den Zutritt zu Gebäuden und Räumen mit IT- bzw. Technikkomponenten.

(2) Im Einzelfall können zusätzliche auftrags- oder systembezogene Sicherheitsverpflichtungen ergänzt werden.

(3) Der Auftragnehmer sorgt innerhalb seines Unternehmens und bei seinen Subunternehmen für die Einhaltung dieser Verpflichtungen.

3. Zutritt Gebäude und Räumlichkeiten

Zutritt zu den Räumlichkeiten/Büros der JUWI-Gruppe sind immer über einen Ansprechpartner bei JUWI zu beantragen. Im Falle, dass dem Auftragnehmer eine Zutrittskarte ausgehändigt wird, ist dieser verpflichtet, diese immer gut sichtbar bei sich zu führen. Dem Auftragnehmer und/oder Mitarbeitende desselben ist es untersagt, sich unbegleitet in Räumlichkeiten der JUWI-Gruppe zu bewegen.

Zweiter Abschnitt – Technische Sicherheitsrichtlinien

4. Zugangs- und Zugriffsrechte

(1) Zugangs- und Zugriffsrechte für das JUWI Netzwerk werden nach Notwendigkeit gewährt und nach Bedarf eingeschränkt. Die Einrichtung von Zugangs- und Zugriffsrechten für das JUWI Netzwerk

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.de

erfolgt durch den JUWI IT-Support per Mail it-support@juwi.de oder per Telefon +4967329657-1111 und muss durch den Auftraggeber für den Auftragnehmer bei diesem beantragt werden.

(2) Vor der Einrichtung von Zugangs- und Zugriffsrechten informiert der Auftragnehmer seine Mitarbeitenden und die Mitarbeitenden seiner Subunternehmen über den Remote Access Antrag und über dieses Dokument „**Informationssicherheit und Datenschutz - Verpflichtungen für IT-Fremddienstleister**“.

(3) Ist für einen Auftragnehmer oder seine Subunternehmen ein Zugang/Zugriff zum JUWI Netzwerk eingerichtet, sind die nachfolgenden Regelungen zu beachten:

- Jede/r Mitarbeitende des Auftragnehmers muss sich mit der von JUWI zugewiesenen Benutzerkennung anmelden. Der Auftraggeber weist den Auftragnehmer hiermit darauf hin, dass Zugang und Zugriffe auf das JUWI Netzwerk protokolliert und ggf. ausgewertet werden. Der Auftragnehmer informiert hierüber seine Mitarbeitenden und Subunternehmen. Benutzerkennungen und Kennwörter dürfen nicht weitergegeben werden.
- Der Auftraggeber ist verpflichtet, den JUWI IT-Support umgehend zu informieren, wenn ein Zugang/Zugriff auf das JUWI Netzwerk nicht mehr erforderlich ist (z.B. Auftragsabschluss, Wechsel Mitarbeitende/r, Kündigung oder sonstige Beendigung des Auftrags). Zugang und Zugriff werden für externe Mitarbeitende auf den Zeitraum der geplanten Dauer des Auftrags, höchsten aber auf sechs (6) Monate befristet.

5. Administrationsrechte

(1) Werden zur Erfüllung des Auftrags durch den Auftragnehmer Administrationsrechte benötigt, können diese nach Anfrage des Auftragnehmers eingerichtet werden.

(2) Die Einrichtung, Änderung und Löschung von Administrationsrechten für Systeme innerhalb des JUWI Netzwerks erfolgt durch den JUWI IT-Support.

(3) Administratoren planen, installieren, konfigurieren und pflegen die informationstechnische Infrastruktur. Sie sorgen im Rahmen ihrer Administrationsaufgaben und -rechte für:

- eine sachgerechte Installation,
- einen störungsfreien Betrieb,
- eine angemessene Pflege der IT-Systeme und Anwendungen und
- Beachtung der Ziele der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) im Verantwortungsbereich.

(4) Der Auftragnehmer bzw. seine Mitarbeitenden und Subunternehmer mit Administrationsrechten haben die folgenden Regeln einzuhalten:

- Die zum Zweck der Erfüllung des Auftrags eingerichteten Administrationsrechte dürfen ausschließlich für den vorgesehenen Zweck verwendet werden. Eine Weitergabe und/oder die Übertragung der zur Erfüllung der Aufgaben persönlich zugeordneten Administrationsrechte sowie diesbezüglicher Benutzerkennungen und Passwörter ist untersagt.
- Werden aus technischen oder organisatorischen Gründen weitergehende Berechtigungen, als für die Erfüllung des Auftrags erforderlich eingerichtet, dürfen dennoch nur die Berechtigungen genutzt werden, die zur Erfüllung des Auftrags zwingend benötigt werden.
- Der unberechtigte bzw. außerhalb des Auftrags liegende Zugang und Zugriff auf IT-Systeme, Dienste, Daten und Anwendungen des Auftraggebers ist untersagt.

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.de

- Das Überwinden von Schutzmaßnahmen und Verschlüsselungsmechanismen ist untersagt.
- Bei der Durchführung von Administrationsaufgaben muss auf eine strikte Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der IT-Systeme, Dienste, Daten und Anwendungen geachtet werden.
- Werden aufgrund von personellen, organisatorischen oder technischen Maßnahmen oder Änderungen die Voraussetzungen der Administrationsrechtevergabe in Teilen oder gänzlich nicht mehr erfüllt oder werden Administrationsrechte nicht mehr benötigt, hat dies der Auftragnehmer unverzüglich dem Auftraggeber mitzuteilen.

6. Schutz des Informationsverkehrs

Werden zur Erfüllung des Auftrags Informationen auf IT-Systemen des Auftragnehmers oder seiner Subunternehmen - außerhalb des JUWI Netzwerks oder in dieses integriert – übertragen und/oder verarbeitet und ggf. mit dem Auftraggeber und/oder Unternehmen der JUWI-Gruppe ausgetauscht, sind zum Schutz der Informationen und des JUWI Netzwerk nachfolgende Schutzmaßnahmen zu beachten:

- Der Auftragnehmer muss sicherstellen, dass auf der von ihm oder seiner Subunternehmen verwendeten und bereitgestellten Hardware (z.B. PCs, Server, Gateways) die aktuellste Version eines anerkannt sicheren Virenschutzsystems mit einer regelmäßig aktualisierten Virensignatur-Datenbank installiert ist, die Schutz gegen Angriffe durch Schadsoftware (z.B. Viren, Würmer, Trojanische Pferde) insbesondere via E-Mail, Web, mobile Datenträger (z.B. USB-Stick) oder anderen Medien bietet, indem sie den Dateizugriff kontrolliert.
- Werden vertrauliche Informationen zwischen dem JUWI Netzwerk und dem Netzwerk des Auftragnehmers oder seiner Subunternehmen ausgetauscht, sind die Informationen nach dem Stand der Technik zu schützen und/oder muss die Übertragung/Transport über eine sichere Verbindung/Transportweg stattfinden. Für den Austausch streng vertraulicher Informationen ist eine Inhaltsverschlüsselung (Container, Hardwareverschlüsselung) und geschützte Übertragung/Transport Pflicht.
- Der Auftragnehmer und seine Subunternehmen müssen über einen definierten Prozess sicherstellen, dass auf der von ihnen verwendeten Hardware korrekt lizenzierte Software und regelmäßig aktualisierte Sicherheits-Patches für die Betriebssystem-Software und die Anwendungen installiert sind.

7. Verbindung zu IT-Systemen

Erfolgt eine Anbindung von IT-Systemen aus Netzen des Auftragnehmers an das JUWI Netzwerk, sind nachfolgende Regelungen zu beachten:

- Wenn zum JUWI Netzwerk Verbindungen hergestellt werden, müssen der Auftragnehmer und seine Subunternehmen sicherstellen, dass ihr eigenes Netzwerk keinen unkontrollierten Zugriff durch Dritte auf das JUWI Netzwerk ermöglicht.
- Der Auftraggeber übernimmt keine Verantwortung für etwaige Schäden an angrenzenden Systemen des Auftragnehmers oder seiner Subunternehmen, die auftreten können, während der Auftragnehmer oder seine Subunternehmen mit dem JUWI Netzwerk verbunden ist.

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.de

8. Verwendung von Wireless-Komponenten

Bei Verwendung von Wireless-Komponenten des Auftragnehmers oder seiner Subunternehmen in Räumlichkeiten der JUWI-Gruppe dürfen bestehende Betriebseinrichtungen nicht beeinträchtigt werden und keine Verbindung zu dem JUWI Netzwerk hergestellt werden.

9. Sicherer System- und Anwendungsbetrieb

Werden IT-Systeme, Anwendungen und IT-Infrastrukturen im Auftrag des Auftraggebers durch den Auftragnehmer in Räumlichkeiten der JUWI-Gruppe oder des Auftragnehmers betrieben und/oder administriert (Anwendungs-Service-Provider), gelten die nachfolgenden Regelungen:

(1) Der Betrieb muss den Anforderungen des Informationsschutzes entsprechen, um als vertrauenswürdig anerkannt zu werden. Hierzu sind insbesondere:
- die gesetzlichen Anforderungen einzuhalten,
- die allgemeingültigen Sicherheitsstandards nach BSI und/oder ISO 27001 zu beachten,
- der Stand der Technik zur sicheren Erhebung, Verarbeitung, Speicherung und Aufbewahrung, Weitergabe sowie Löschung/Entsorgung schutzwürdiger Informationen und
- die Anforderungen an Kommunikations- und Eskalationsprozesse bezogen auf Informationsschutz relevante Ereignisse zu beachten.

(2) Der Auftragnehmer und seine Subunternehmen müssen angemessene Vorsichtsmaßnahmen treffen, um die Hardware-Komponenten vor physischen Schäden zu schützen und die Verwendung durch unbefugte Benutzer zu verhindern.

(3) Der Auftragnehmer und seine Subunternehmen müssen die Sicherheit der Betriebsumgebung gewährleisten sowie logische Zugangs- und Zugriffskontrollen implementieren.

(4) Beinhaltet der Auftrag die Erhebung, Nutzung oder Verarbeitung personenbezogener Daten im Sinne der Datenschutzgrundverordnung und des Bundesdatenschutzgesetzes, muss der Auftragnehmer alle aufgrund der gesetzlichen Vorgaben erforderlichen Maßnahmen zum Schutz der Daten treffen.

10. Software Entwicklung und Integration

Erbringt der Auftragnehmer Leistungen der Softwareentwicklung und/oder -integration, sind unter Beachtung dieses Dokuments die projektspezifischen Sicherheitsanforderungen umzusetzen, die zwischen Auftraggeber und Auftragnehmer gesondert vereinbart werden.

Dritter Abschnitt – Allgemeine Verpflichtungen

11. Nutzung von Informationen des Auftraggebers

(1) Der Auftragnehmer und seine Subunternehmen sind verpflichtet, die vom Auftraggeber eingeräumten Zutrittsrechte sowie Zugangs- und Zugriffsrechte (IT-Systeme, Dienste, Daten und Anwendungen) ausschließlich im Rahmen der vertraglich zu erfüllenden Verpflichtungen zu nutzen.

(2) Sämtliche durch den Auftrag erlangte, nicht öffentlich bekannte Informationen sowie auftragsbedingt erstellte Kopien, Aufzeichnungen und Arbeitsergebnisse sind Eigentum des Auftraggebers und an diesen nach Beendigung des Auftrages heraus bzw. zurückzugeben.

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.de

(3) Der Auftragnehmer und seine Subunternehmen sind verpflichtet, alle im Zusammenhang mit der Vertragserfüllung zur Kenntnis gelangten Informationen über den Auftraggeber und Unternehmen der JUWI-Gruppe, ihre Geschäfts- und Betriebsangelegenheiten und alle Arbeitsergebnisse vertraulich zu behandeln und angemessen gegen eine Kenntnisnahme durch Unberechtigte und nicht vertragsgemäße Nutzung, Vervielfältigung oder Weitergabe zu schützen. Diese Verpflichtungen gelten über die Beendigung des Vertragsverhältnisses hinaus.

(4) Dem Auftragnehmer und seinen Subunternehmen ist nicht gestattet, sich geschäftliche oder betriebliche, nicht von der JUWI-Gruppe öffentlich bekannt gemachte Informationen gleich welcher Art über Auftraggeber und/oder seine Kunden, Lieferanten oder Mitarbeiter anzueignen, für eigene Zwecke zu nutzen oder Kopien oder Aufzeichnungen irgendwelcher Art zu fertigen, soweit dies nicht zur Erfüllung des Auftrags erforderlich ist. Solche Informationen, Kopien, Aufzeichnungen oder Arbeitsergebnisse dürfen auch nicht an Dritte weitergegeben oder Dritten zur Kenntnis gebracht werden.

(5) Vertrauliche Informationen dürfen nur an die Subunternehmen weitergegeben werden, für die der Auftraggeber seine Zustimmung erteilt hat und die auf die Einhaltung dieses Dokuments „**Informationssicherheit und Datenschutz - Verpflichtungen für IT-Fremddienstleister**“ verpflichtet wurden.

12. Datenschutz

(1) Der Auftragnehmer leistet Gewähr, dass er sämtliche geltenden Datenschutzgesetze, namentlich die EU-Datenschutzgrundverordnung (DSGVO) und das Bundesdatenschutzgesetz 2018 (BDSG) befolgt und dass er alle nach geltendem Recht erforderlichen Genehmigungen im Hinblick auf den Umgang und/oder die Handhabe personenbezogener Daten eingeholt hat. Der Auftragnehmer wird den Auftraggeber von allen Kosten, Ansprüchen, Haftungen und Forderungen freistellen, die dem Auftraggeber im Hinblick auf eine Verletzung dieser Gewährleistung entstehen.

(2) Mit der Beauftragung wird der Auftragnehmer darauf hingewiesen, dass die „**Hinweise zur Datenverarbeitung für Kunden, Lieferanten und andere Betroffene**“ des Auftraggebers zu beachten sind. Der Auftragnehmer verpflichtet sich hiermit für den Fall, dass der Betroffene nicht zugleich der Auftragnehmer ist, diese „Hinweise zur Datenverarbeitung für Kunden, Lieferanten und andere Betroffene“ an die Betroffenen weiterzugeben, die im Rahmen dieses Vertragsverhältnisses auf Initiative des Auftragnehmers mit dem Auftraggeber Kontakt haben werden.

(3) Sofern der Auftragnehmer im Rahmen dieses Vertragsverhältnisses als Auftragsverarbeiter im Sinne des Art. 28 DSGVO tätig wird, werden Auftragnehmer und Auftraggeber zuvor eine den gesetzlichen Vorgaben genügende Vereinbarung zur Auftragsverarbeitung abschließen. Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftragnehmer und Auftraggeber als Gesamtschuldner. Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenen Umstandes ist, soweit die relevanten Daten unter dieser Vereinbarung erarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von sämtlichen Ansprüchen, Forderungen, Haftungen Dritter bzw. gegenüber Dritten sowie Kosten frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeitenden bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm

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.de

eingesetzten Subunternehmer im Zusammenhang mit der Erbringung der beauftragten Leistung schuldhaft verursachen. Dieser Punkt 12 gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Leistungen oder einer vom Auftraggeber erteilten Weisung entstanden ist.

(4) Der Auftragnehmer verpflichtet sich, nur Mitarbeitende einzusetzen, die auf das Datengeheimnis gemäß § 5 BDSG (alt) oder zur Wahrung der Vertraulichkeit im Sinne der DSGVO verpflichtet wurden und diese Verpflichtung auch für die Zeit nach ihrem Ausscheiden aus dem Arbeitsverhältnis mit dem Auftragnehmer gilt.

(5) Eine Weitergabe personenbezogener Daten des Auftraggebers durch den Auftragnehmer an Dritte (einschließlich von Subunternehmern) bedarf ungeachtet der gesetzlichen Voraussetzungen in jedem Fall der vorherigen schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer verpflichtet sich, Subunternehmer nur dann mit der Verarbeitung von personenbezogenen Daten des Auftraggebers zu betrauen, wenn diese sich zuvor schriftlich in gleicher Weise wie der Auftragnehmer zur Einhaltung der Verpflichtungen nach diesem Punkt 12 „Datenschutz“ verpflichtet haben.

13. Persönliche Eignung und fachliche Qualifikation der Mitarbeitenden

(1) Der Auftragnehmer ist verpflichtet, ausschließlich Mitarbeitende beim Auftraggeber einzusetzen, die persönlich geeignet und fachlich qualifiziert sind. Die Beurteilung der Mitarbeitenden ist vor Beginn des Auftragsverhältnisses durch den Auftragnehmer sicherzustellen.

(2) Auf Anfrage des Auftraggebers weist der Auftragnehmer dem Auftraggeber mittels geeigneter Unterlagen, die fachliche Eignung der jeweils eingesetzten Mitarbeitenden nach.

(3) Die Absätze 1 und 2 gelten entsprechend für Mitarbeitende von Nachunternehmen des Auftragnehmers.

Vierter Abschnitt – Kontrolle der Einhaltung der Sicherheitsrichtlinien, Meldepflicht und Zugangs- und Zugriffssperrung

14. Kontrolle, Meldepflicht und Zugriffssperre

(1) Der Auftraggeber hat das Recht, die Einhaltung dieses Dokuments auch am Standort des Auftragnehmers zu kontrollieren.

(2) Der Auftragnehmer ermöglicht dem Auftraggeber insbesondere nach vorheriger Benachrichtigung und innerhalb der normalen Geschäftszeiten Zutritt zu allen relevanten Betriebsstandorten und unterstützt ihn bei allen erforderlichen Aktivitäten und Tests. Er gewährt darüber hinaus Einsicht in, für das JUWI Netzwerk betriebsrelevante Dokumentation.

(3) Des Weiteren behält sich der Auftraggeber das Recht vor, die Art des Zugangs/Zutritts des Auftragnehmers und/oder seiner Subunternehmen auf das JUWI Netzwerk zu modifizieren, um die Sicherheit des JUWI Netzwerks zu gewährleisten.

(4) Der Auftragnehmer ist verpflichtet, die für ihn einschlägigen Sicherheitsregelungen und Gesetze einzuhalten, sämtliche relevanten Fehler, Unregelmäßigkeiten oder Sicherheitsvorfälle sowie eingeleitete Maßnahmen zu deren Behebung im Zusammenhang mit dem JUWI Netzwerk revisionssicher zu dokumentieren und dem Auftraggeber unverzüglich zu melden.

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.de