Handlungsleitlinie zu Datenschutz und Informations-sicherheit für Auftragnehmer der EXXETA

(Stand: 01.10.2019)

1. Geltungsbereich

Nur aufgrund ihrer vertraglichen Aufgaben sind die von EXXETA beauftragten Unternehmen, deren Mitarbeiter und die als Selbständige für EXXETA tätigen Personen (im Folgenden zusammengefasst als „Auftragnehmer“ bezeichnet) befugt, die Informationen und IT-Ressourcen der EXXETA oder ihrer Kunden zu nutzen. Alle von EXXETA beauftragten Auftragnehmer sind deshalb durch den geschlossenen Einzelvertrag zur Einhaltung dieser Handlungsleitlinie verpflichtet und müssen sicherstellen, dass auch ihre Mitarbeiter, Verrichtungs- und Erfüllungsgehilfen (im Folgenden zusammengefasst als „Mitarbeiter“ bezeichnet) vor Aufnahme ihrer Tätigkeit informiert wurden und entsprechend verpflichtet sind.

Die in dieser Handlungsleitlinie dokumentierten Regeln können in weiteren konkretisierten Handlungsanweisungen detailliert und erweitert werden. Die hier definierten Regeln sind als Mindeststandard einzuhalten. Soweit der Auftragnehmer Zugriff auf Daten, Informationen, Systeme oder einen Zugangsausweis zu den Geschäftsräumen der EXXETA oder ihrer Kunden erhält, können dem Auftragnehmer weitere Verpflichtungserklärungen vorgelegt werden, die von ihm und ggf. seinen Mitarbeitern persönlich zu unterzeichnen sind. Der Auftragnehmer wird EXXETA die entsprechend unterzeichneten Formulare unverzüglich vorlegen. Ein Einsatz von Personen, die diese Verpflichtungserklärungen nicht unterzeichnet haben, ist unzulässig.

Kunden schließen mit EXXETA regelmäßig zusätzliche Vereinbarungen zu Datenschutz und Informationssicherheit, die sowohl EXXETA als auch ihre Auftragnehmer verpflichten. In diesem Fall gehen die Regelungen jener Vereinbarung im Fall von Widersprüchen den Regelungen in dieser Richtlinie vor.

2. Grundlegende Anforderungen an Datenschutz und Sicherheit

Der Auftragnehmer darf bei der Erfüllung des Vertrages nur Personen einsetzen, die auf Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr.1 DSGVO vorverpflichtet und belehrt sind sowie die im Rahmen der Beauftragung Datenschutzbestimmungen und Datensicherheitsmaßnahmen beachten. Insbesondere müssen diese Personen darüber informiert sein, personenbezogene Daten nur innerhalb der übertragenen Aufgaben zu verarbeiten und personenbezogene Daten nicht unbefugt zu erheben, zu verarbeiten, bekanntzugeben, zu übermitteln, zugänglich zu machen oder sonst zu verwenden. Bei der Verarbeitung personenbezogener Daten sind darüber hinaus die Bestimmungen der DSGVO einzuhalten.
Soweit der Auftragnehmer aufgabenbedingt an der Erbringung von Telekommunikations-dienstleistungen mitwirkt, wird er gemäß Telekommunikationsgesetz das Fernmeldegeheimnis (§ 88 TKG) wahren und niemandem eine Kenntnisnahme von Gesprächsdaten bzw. -inhalten ermöglichen oder verschaffen und diese unbefugt verwenden.
Datenschutzrechtlich relevante Vorkommnisse sind umgehend an Datenschutz@EXXETA.com zu melden.

3. Grundlegende Anforderungen an die Informationssicherheit

Ziel der Informationssicherheit ist es, den Geschäftsbetrieb der EXXETA bzw. ihrer Kunden sicherzustellen und das Risiko eines Schadens durch die Verhütung von Sicherheitsvorfällen und die Reduzierung ihrer potenziellen Auswirkungen zu minimieren. Die Gesamtheit aller Maßnahmen dient dem Erhalt von Vertraulichkeit, Integrität und Verfügbarkeit der Informationen. Es ist deshalb von entscheidender Bedeutung, dass sich jeder Mitarbeiter des Auftragnehmers seiner Pflichten in Bezug auf Informationssicherheit und Datenschutz bewusst ist.

Die Einhaltung der Sicherheitsrichtlinie stellt sicher, dass:

- Informationen gegen alle nicht autorisierten Zugriffe geschützt werden,
- die Vertraulichkeit und Integrität der Informationen geschützt werden,

- die Verfügbarkeit von Informationen für Geschäftsprozesse gewährleistet ist,
- alle tatsächlichen oder vermuteten Informationssicherheitsverletzungen dem Informations-sicherheitsbeauftragten gemeldet und gründlich untersucht werden
- und gesetzliche Auflagen eingehalten werden.

Informationen sind insbesondere, aber nicht ausschließlich

- sämtliche nicht-öffentlichen Informationen (interne, vertrauliche und streng vertrauliche Informationen)
- ausgedruckte und elektronische Dokumente sowie Kopien
- Konzepte, Pläne und Arbeitsergebnisse
- Verfahrensweisen und Quellcodes
- sonstige Geheimnisse

Der Auftragnehmer verpflichtet sich, sämtliche Informationen zu schützen, sofern diese nicht-öffentlicher Natur sind. Zu diesem Zweck wird der Auftragnehmer Informationen, die er im Laufe der Zusammenarbeit direkt oder indirekt erhalten hat, vertraulich behandeln, für keinen anderen Zweck als zur Erfüllung der im Vertrag festgelegten Pflichten verwenden und vor unerlaubter Vervielfältigung, Verbreitung oder Nutzung zu schützen. Solche Informationen sind mit derselben Sorgfalt zu behandeln, mit der eigene vertrauliche Informationen bzw. vertrauliche Informationen eines ordentlichen Kaufmanns behandelt werden. Der Auftragnehmer hat insbesondere angemessene Vorkehrungen zu treffen, um die Informationssicherheit innerhalb seines Zuständigkeitsbereichs zu gewährleisten. Auf Anfrage der EXXETA wird der Auftragnehmer entsprechende Maßnahmen schriftlich nachweisen.

Der Auftragnehmer gewährleistet, dass seine Mitarbeiter entsprechende Trainings zu Datenschutz und Informationssicherheit erhalten, um sicherzustellen, dass sie über angemessene Kenntnisse und Fähigkeiten verfügen, um Informationen im erforderlichen Umfang zu schützen. Der Auftragnehmer wird sie über die Folgen bei einem Verstoß gegen die Regelungen in dieser Richtlinie und die geltenden Sicherheitsanforderungen informieren

Der Auftragnehmer hat EXETA bzw. ihren Kunden sofort und ohne schuldhafte Verzögerung über jede unrechtmäßige Offenlegung, Verwendung oder Missbrauch von Informationen ungeachtet der Person zu informieren.

4. Sicherheitsstandards

4.1 Der Auftragnehmer benennt EXXETA mindestens eine verantwortliche Person, die entscheidungsbefugt für IT-sicherheitsrelevante Fragestellungen ist.

4.2 Der Auftragnehmer stellt sicher, dass die von EXXETA oder ihrem Kunden vorgegebenen Entwicklungsrichtlinien und Sicherheitsvorschriften eingehalten werden.

4.3 Auf Grund des hohen Schutzbedürfnisses der Daten ist der Zugriff und die Verarbeitung und Nutzung aller Daten nur mit von EXXETA oder ihrem Kunden dafür vorgesehenen technischen Mitteln erlaubt. Der Auftragnehmer sorgt dafür, dass ein Zugriff auf IT-Systeme von EXXETA oder deren Kunden im Rahmen der Leistungserbringung nur von mit entsprechenden Zugriffsberechtigungen ausgestatteten Personen erfolgt. Die Weitergabe von Zugangsdaten (z.B. Passwörter) zum Zugriff auf solche IT-Systeme an Dritte ist nur mit schriftlicher vorheriger Zustimmung von EXXETA zulässig. Sobald ein Mitarbeiter nicht mehr mit der Auftragserfüllung befasst ist, hat der Auftragnehmer dies EXXETA unverzüglich anzuzeigen. Ab diesem Zeitpunkt ist eine Zustimmung im Sinne dieser Vorschrift für seine Person ebenfalls erforderlich. Eine Zugriffsberechtigung besteht indes nicht mehr.

4.4 Alle IT-/EDV-Geräte, -Datenträger und -Software, die dem Auftragnehmer zur Verfügung gestellt werden sind nur zur definierten Aufgabenerfüllung bestimmt. Weiterhin sind diese vor unbefugtem Zugriff (durch Sperren, Absperren und/oder Verschlüsseln) stets zu schützen. Hardware darf nur nach vorheriger Zustimmung und in Abstimmung mit EXXETA oder ihrem

Kunden aus deren Räumlichkeiten entfernt werden. Sie dürfen nur von den Mitarbeitern benutzt werden, für die sie ausgegeben bzw. installiert wurden. Dies gilt nur solange der Mitarbeiter an der Aufgabenerfüllung beteiligt ist. Jede Änderung an den EDV-Geräten ist unzulässig. Sicherheitsupdates für Betriebssysteme und Anwendungsprogramme sind unverzüglich zu installieren. Bei Smartphones oder Tablets sind SIM-Karte und Gerät vor fremdem Zugriff zu schützen.

4.5 Sofern der Auftragnehmer zur Erbringung der Leistung eigene IT-Systeme, Geräte oder Datenträger einsetzt, in denen Daten EXXETAs bzw. dessen Kunden verarbeitet werden, so sind für die Authentisierung von Benutzern am Gerät, Datenträger, Netzwerk bzw. an dem relevanten IT-System des Auftragnehmers angemessene Passwörter zu benutzen. Insbesondere sind durch den Auftragnehmer die Passwortlänge (mindesten zehn Zeichen), die Anzahl der zu nutzenden Zeichentypen, die maximale Gültigkeit und die Komplexität der Passwörter zu regeln. Datenspeicher sind entsprechend den Vorgaben von EXXETA bzw. des Kunden zu verschlüsseln.

4.6 Softwareprodukte dürfen, sofern im Einzelfall nichts anderes bekannt gegeben wird, nur an dem Gerät benutzt werden, für das sie zur Verfügung gestellt bzw. an dem sie installiert wurden und dürfen nur für die Zwecke genutzt werden, für die sie beantragt und genehmigt wurden. Kopieren ist nur im Sinne der Daten- und Programmsicherung - und nur unverändert - erlaubt.

4.7 Fremde Datenträger sind vor dem erstmaligen Verwenden auf Viren zu prüfen. Verdächtige Mails und Anrufe sind umgehend gemäß Kapitel 6 zu melden und dokumentieren. Bei Auftreten eines Virus muss der IT-Sicherheitsbeauftragte unverzüglich informiert werden, bevor am System weitergearbeitet werden darf. Das Umgehen dieser Schutzmaßnahmen ist verboten.

4.8 Für Remote-Zugänge müssen verschlüsselte VPN Verbindungen genutzt werden. Für Zugang zum EXXETA Netzwerk darf dies nur durch von EXXETA freigegebene Hardware erfolgen.

4.9 Der Auftragnehmer hat dafür Sorge zu tragen, dass seine Mitarbeiter die Besuchsbedingungen und Hausordnung der EXXETA oder ihrem Kunden beachten. Schwere Verstöße gegen die Besuchsbedingungen oder die Hausordnung berechtigen zur Verhängung eines Hausverbots gegen einzelne Mitarbeiter des Auftragnehmers.

4.10 Der Auftragnehmer ist zum Schutz des Eigentums EXXETAs und ihres Kunden verpflichtet. Zum Eigentum zählen alle Sach- und Vermögenswerte, das geistige Eigentum sowie die Inhaberschaft von Rechten. Bei Verlust oder Diebstahl von IT-Geräten ist EXXETA unverzüglich zu informieren.

4.11 Bei Vertragsende müssen alle Geräte umgehend zurückgegeben werden; dies hat an der Ausgabestelle zu erfolgen, alternativ in den großen EXXETA-Standorten beim Empfang, sonst per versichertem Paket.

4.12 Beim Transport von Hardware per Auto darf diese nicht über Nacht im Auto verbleiben. Ebenfalls darf die Hardware nicht sichtbar im Auto liegen gelassen werden.

4.13 Für die Entsorgung von sensiblen Unterlagen sind die von EXXETA bzw. ihrem Kunden zur Verfügung gestellten Aktenvernichter bzw. Datenschutztonnen zu verwenden.

5. Verbote

5.1 Jede schuldhaft ermöglichte Nutzung der durch EXXETA oder ihres Kunden zur Verfügung gestellten Kommunikationsmittel (bspw. E-Mail, Telefon, Internet), die geeignet ist, dem Interesse und dem Ansehen EXXETAs oder ihrer Kunden in der Öffentlichkeit zu schaden, die Informationssicherheit zu gefährden oder gegen geltende Rechtsvorschriften sowie vorhandene Anweisungen, Richtlinien oder Vereinbarungen verstößt, ist unzulässig.

5.2 Nicht erlaubt ist darüber hinaus:

- Das Abrufen, Verbreiten oder Speichern von illegalen Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen;
- Das Abrufen, Verbreiten oder Speichern von beleidigenden, übel nachredenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, Gewalt verherrlichenden oder pornografischen Äußerungen oder Abbildungen;
- Die private Nutzung der geschäftlichen E-Mail-Adresse (falls von EXXETA oder ihrem Kunden zur Verfügung gestellt);
- Der Einsatz von Funktastaturen und Funkmäusen, sofern diese nicht mindestens eine 128-Bit-AES Verschlüsselung und die aktuelle Firmware des Herstellers verwenden. Es dürfen nur durch EXXETA oder ihrer Kunden gestellte Eingabegeräte genutzt werden;
- Das Kopieren und/oder Installieren von Software, für die keine gültige Lizenz vorliegt. Sofern Software für den geschäftlichen Gebrauch eingesetzt werden soll, ist hierfür in Abstimmung mit EXXETA bzw. ihrem Kunden eine Lizenz anzufordern;
- Das Speichern von privaten Daten auf Servern von EXXETA oder ihrer Kunden;
- Personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu erheben, zu verarbeiten, zugänglich zu machen oder sonst zu nutzen. Diese Verpflichtung besteht über den Anstellungszeitraum hinaus;
- Die Vermischung oder Verbindung von geschäftlichen und privaten Daten. Sofern EXXETA oder ihr Kunde für die Auftragserfüllung es vorschreibt, ist dessen MDM-Lösung einzusetzen;
- Ohne Absprache mit EXXETA bzw. ihres Kunden Veränderungen an der Konfiguration des Virenscanners, der Firewall und der Festplattenverschlüsselung bei dienstlich bereitgestellten Geräten vorzunehmen;
- Ohne Absprache das vorinstallierte Betriebssystem von dienstlich bereitgestellten Geräten zu entfernen; dies verbietet auch "rooten" und "jailbreak";
- Die Übermittlung, Verarbeitung und Speicherung von geschäftlichen, personenbezogenen Daten Dritter außerhalb des Verantwortungsbereichs von EXXETA bzw. des Kunden (z.B. Hochladen von personenbezogenen Daten zu einem nicht von EXXETA freigegebenen externen Cloud-Anbieter wie Apple iCloud oder Google Drive oder Dropbox);
- Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist nur nach Freigabe durch EXXETA oder ihres Kunden zulässig. Hierzu zählen beispielsweise Netzwerksniffer;
- Die Weitergabe von Passwörtern, Zugangsdaten, Zertifikaten und WLAN-Schlüsseln (außer Gäste-WLAN) an Dritte;
- Die Aufnahme privater Geräte in das Netzwerk der EXXETA oder ihres Kunden ohne Absprache mit der IT / dem Netzwerkadministrator;
- Für Mitarbeiter in sensiblen Abteilungen lokalen Administrationsrechte zu vergeben. Vorhandene Berechtigungen sind zu entziehen.

6. Behandlung von Sicherheitsvorfällen

Wenn der Verdacht besteht, dass die Vertraulichkeit oder die Integrität eines zur Erbringung der Leistung beteiligten IT-Systems verletzt worden ist bzw. die Verfügbarkeit eines solchen IT-Systems aufgrund eines externen oder internen Angriffes beeinträchtigt worden ist, ist EXXETA bzw. ihr Kunden grundsätzlich und schnellstmöglich durch den Auftragnehmer zu benachrichtigen. Meldungen an EXXETA sind per E-Mail an infosec@exxeta.com zu schicken.

7. Folgen eines Verstoßes

Fahrlässige und vorsätzliche Verstöße gegen die Vorschriften zu Datenschutz und Informationssicherheit können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe nach den gesetzlichen Vorschriften geahndet werden. Entsteht einer betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen.