Richtlinie für externe Dienstleister bei Zugriff auf TRILUX IT Systeme

1. Geltungsbereich

Die Unternehmen der TRILUX Gruppe (s. Unternehmensliste auf www.trilux.com oder die auf Anfrage zur Verfügung gestellt wird) beauftragen, zur Erbringung von IT-Services (Beratung, Anwendungsentwicklung und Betrieb), externe IT-Dienstleister unter anderem auch durch externe Kommunikationsverbindungen („Remote-Zugriff"). Die hierbei erforderliche Nutzung der informationstechnischen Systemen durch externe Anwender unterliegt den nachstehenden Regelungen als Mindestanforderung für eine Dienstleistungserbringung und werden mit der Unterzeichnung/Kenntnisnahme Bestandteil des/der mit dem Dienstleister bestehenden Vertrages/Geschäftsbeziehung.

2. Generelle Regelungen des Datenzugangs, IT Sicherheit

2.1. Der Dienstleister hat jederzeit sicher zu stellen, dass seine Handlungen nicht die Verfügbarkeit, Integrität oder Vertraulichkeit von IT-Systemen beeinträchtigen. Er führt ausschließlich die Tätigkeiten durch, die zur Erfüllung der beauftragten Leistungen erforderlich sind. Er führt sie ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Änderungen des Tätigkeitsfeldes und Verfahrensänderungen sind schriftlich zu vereinbaren. Eine Verarbeitung erfolgt nur, soweit es im zugrunde liegenden Leistungsvertrag vereinbart ist.

2.2. Informationen, Daten und Programme dürfen lediglich im Rahmen der Erfüllung der vereinbarten Tätigkeiten und nach der Genehmigung durch den Auftraggeber von oder aus der Infrastruktur des Auftraggebers übertragen bzw. installiert werden.

2.3. Der Zugriff darf nur von Systemen aus erfolgen, deren Sicherheitsniveau den Vorgaben der Informationssicherheit beim Auftraggeber entspricht.

2.4. Der Dienstleister sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

2.5. Der Dienstleister hat in geeigneter Weise an der Erstellung der Verfahrensbeschreibungen mitzuwirken, wenn dies im Rahmen der vertraglichen Leistungserbringung vorgeschrieben ist oder vom Auftraggeber gewünscht wird.

2.6. Der Dienstleister beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

2.7. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt der Dienstleister den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen, Verstöße des Dienstleisters oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

2.8. Der Dienstleister wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt.

2.9. Der Dienstleister teilt dem Auftraggeber mit, welche Mitarbeiter er zur Erfüllung der Tätigkeiten einsetzt und wie sich diese identifizieren werden. Hierfür werden hinreichend sichere Identifizierungsverfahren verwendet, die entsprechend zu schützen sind. Sollten die Identifizierungsmerkmale offengelegt werden, ist der Auftraggeber unverzüglich hierüber zu informieren.

2.10. Der Dienstleister stellt sicher, dass die Infrastruktur des Auftraggebers nicht durch seine Tätigkeiten negativ beeinflusst wird. Unter negativer Beeinflussung ist das unregelmäßige, abnormale Verhalten der Infrastruktur zu verstehen, das zu einem Versagen einzelner Komponenten oder des gesamten Systems führt und der Dienstleister verschuldet hat.

2.11. Nach Abschluss der vertraglichen Arbeiten hat der Dienstleister sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Dienstleisters sind danach physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen.

2.12. Der Dienstleister hat einen Mitarbeiter benannt, der für alle IT-Sicherheitsaspekte der Dienstleistungserbringung verantwortlich ist.

3. Zugriff, Auditrecht

3.1. Der Auftraggeber wird dem Dienstleister nur die für die Durchführung der vereinbarten Tätigkeiten benötigten Zugriffsrechte bereitstellen, deren Aktualität regelmäßig überprüfen und gegebenenfalls Korrekturen vornehmen. Der Dienstleister darf von den ihm eingeräumten Zugriffsrechten nur in dem für die Durchführung der Tätigkeiten unerlässlich notwendigen Umfang Gebrauch machen.

3.2. Der Auftraggeber hat das Recht, den Zugriff des Dienstleisters auf die informationstechnischen Systeme des Auftraggebers zu unterbrechen.

3.3. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften aus dieser Vereinbarung im erforderlichen Umfang zu kontrollieren oder kontrollieren zu lassen. Der Dienstleister gewährt dazu nach Absprache ungehinderten Zutritt, Zugang und Zugriff zu informationsverarbeitenden Systemen, Programmen, Dateien und Informationen, die mit der Durchführung der Tätigkeiten in Verbindung stehen. Dem Auftraggeber sind durch den Auftragnehmer alle Auskünfte zu erteilen, die zur Erfüllung der Kontrollfunktion benötigt werden.

3.4. Der Auftraggeber ist berechtigt, sämtliche Aktionen des Dienstleisters innerhalb seiner Infrastruktur zu protokollieren und auszuwerten.

4. Mitarbeiter und Subunternehmer des Dienstleisters

4.1. Der Dienstleister darf Subunternehmer lediglich nach schriftlicher Genehmigung durch den Auftraggeber im Rahmen der Erfüllung der vertraglich beauftragten Tätigkeiten einsetzen. Der Dienstleister ist für die Handlungen oder Unterlassungen seiner Subunternehmer auf die gleiche Weise wie für seine eigenen Handlungen oder Unterlassungen verantwortlich.

4.2. Der Dienstleister steht dafür ein, dass die Inhalte dieser Richtlinie allen Mitarbeitern und gemäß Ziffer 4.1 genehmigten Subunternehmern, die einen Zugriff auf Informationen des Auftraggebers bekommen bekannt sind und wird die in ANLAGE 1

aufgeführte Arbeitsanweisung mit jedem der Arbeitnehmer/Subunternehmer treffen, die Zugriff auf die IT Systeme des Auftraggebers erhalten.

5. Vertraulichkeit

5.1. Der Dienstleister ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln, auch über das Vertragsende hinaus. Sich gegebenenfalls aus der Vertragsbeziehung ergebende allgemeine oder weitergehende Geheimhaltungsverpflichtungen werden durch diese Erklärung nicht berührt.

5.2. Unverzüglich nach der schriftlichen Aufforderung durch den Auftraggeber von dem Dienstleister sind alle ihm vorliegenden vertraulichen Informationen und aufgrund dieser Informationen gefertigten weiteren Unterlagen, dem Auftraggeber zurückzusenden bzw. nachvollziehbar zu vernichten.

6. Datenschutz

6.1. Der Dienstleister stellt unter Wahrung der Verhältnismäßigkeit alle organisatorischen und technischen Maßnahmen zum Schutz personenbezogener Daten gem. Art. 32 DS-GVO sicher.

6.2. Beim Auftraggeber ist der ordnungsgemäß bestellte Datenschutzbeauftragte unter privacy@trilux.com zu erreichen. Der Dienstleister hat, sofern er gesetzlich hierzu verpflichtet ist, einen Datenschutzbeauftragten bestellt und teilt dessen Kontaktdaten auf Anfrage unverzüglich mit. Ein Wechsel des Datenschutzbeauftragten haben sich die Parteien unverzüglich mitzuteilen.

6.3. Über datenschutzrelevante Vorfälle und Verstöße gegen die vertraglichen Regelungen unterrichtet der Dienstleister den Auftraggeber schriftlich und unverzüglich.

6.4. Notwendige Datenübertragungen zu Zwecken des Zugriffs müssen in hinreichend verschlüsselter Form erfolgen; Ausnahmen sind besonders zu begründen.

6.5. Die Verarbeitung und Speicherung der Daten findet ausschließlich im Gebiet der Europäischen Union statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44–49 DS-GVO erfüllt sind. Falls ein Unterauftragnehmer beauftragt werden soll, gelten diese Anforderungen zusätzlich zu den Bestimmungen in Abs. 13 dieser Vereinbarung.

7. IT gestützte Kommunikation & Austausch von Daten

7.1. Zur Erleichterung der auftragsbezogenen Kommunikation und dem Austausch von Daten können Zugänge und Freigaben innerhalb der TRILUX Domain eingerichtet werden.

7.2. Die Nutzung der Plattformen ist ausschließlich im Zusammenhang mit dem Auftrag gestattet. Eine private Nutzung ist nicht gestattet.

7.3. Die Weitergabe von Daten an Dritte oder private Ablageorte ist nicht gestattet. Ausnahmen sind ausdrücklich zu genehmigen.

ANLAGE 1 Arbeitsanweisung Fernwartung/Nutzung TRILUX IT Systeme

- Der Mitarbeiter des Dienstleisters erhält nach vorheriger Beauftragung einen persönlichen Zutritt zu Datenverarbeitungsanlagen, sofern es im Rahmen der Aufgabenerfüllung notwendig ist. Die Zutrittsberechtigung ist nicht auf Dritte übertragbar.
- Der Mitarbeiter des Dienstleisters erhält zur Aufgabenerfüllung einen Zugang zu den Datenverarbeitungssystemen. Dieser besteht aus einer eindeutigen, persönlichen Benutzerkennung und einem Passwort. Zusätzlich erhält der Mitarbeiter des Dienstleisters einen Zugang zur Fernanmeldung.
- Für das Passwort gelten die folgenden Komplexitätsanforderungen, die auch bei einer Änderung zu berücksichtigen sind. Das Initialpasswort muss bei der ersten Anmeldung und danach alle 90Tage geändert werden. Das Passwort
  - enthält keine logische Zeichenfolge (z. B. Abfolge direkt benachbarter Zeichen auf der Tastatur),
  - lässt sich nicht leicht erraten oder ableiten (z. B. Lebensmittel, Musik, Wörterbuchbegriffe),
  - nutzt Groß- und Kleinschreibung,
  - hat zwölf Zeichen als Mindestlänge,
  - nutzt Ziffern (0–9),
  - nutzt Sonderzeichen (z. B. &, §, >, #).
- Sollte es zu Problemen oder technischem Fehlverhalten kommen, ist der Helpdesk des Auftraggebers hierüber unverzüglich zu informieren. Der Helpdesk unterstützt bei der Lösung und steht bei Fragen zur Anmeldung zur Verfügung. Er ist zu erreichen unter folgenden Kontaktdaten: **+49(0)2932/301-444** / helpdesk@helpdesk.trilux.de
- Der Zugriff auf Unternehmensressourcen darf lediglich im Rahmen des Vertrages erfolgen. Die entsprechenden Zugriffsrechte werden durch den Auftraggeber vergeben. Ein Zugriff auf nicht benötigte Informationen ist untersagt. Sollte dem Mitarbeiter des Dienstleisters auffallen, dass Zugriffsberechtigungen falsch vergeben sind, so ist dies unverzüglich dem Auftraggeber mitzuteilen. Dieser veranlasst umgehend eine Anpassung der Zugriffsberechtigungen. Die Ausnutzung fehlerhafter Zugriffsberechtigungen ist untersagt.
- Sollte die Zugangsprüfung nicht auf andere Weise erfolgen (z. B. Active Directory, Single Sign On), sind für unterschiedliche Anwendungen unterschiedliche Passwörter zu verwenden. Passwörter, die zur Anmeldung bei Dienstleistern im Internet genutzt werden, dürfen nicht zur Anmeldung am Netzwerk des Auftraggebers verwendet werden. Passwörter sind unbeobachtet einzugeben. Für diese Identifikationsmerkmale gilt, dass eine Veröffentlichung, Weitergabe oder missbräuchliche Nutzung ausdrücklich untersagt ist. In Anwendungen vorhandene Funktionen zur Passwortspeicherung sind nicht zu verwenden. Ebenso ist das Niederschreiben der Benutzerkennung und des Passwortes untersagt. Besteht die Notwendigkeit der Speicherung von Passwörtern, kann ein Passwort-Safe genutzt werden.