

CHARTA

für IT-Sicherheit & Datenschutz

IT-Sicherheit und Datenschutz sind für den Unternehmenserfolg von Circet Switzerland unverzichtbar. Der Schutz von persönlichen, Unternehmens- und Kundendaten muss durch die Subunternehmer sowie Lieferanten jederzeit gewährleistet werden.

1. IT-SICHERHEIT

Das Informationssystem (IS) von Circet Switzerland bietet eine Vielzahl von Ressourcen und Geräten, die den Benutzern zur Erfüllung ihrer beruflichen Aufgaben zur Verfügung stehen. Circet Switzerland legt grossen Wert darauf, angemessene Massnahmen zu definieren und umzusetzen, damit ein reibungsloser Betrieb sowie die Sicherheit ihres IS gewährleistet ist. Circet Switzerland erwartet von den Subunternehmen und Lieferanten, dass ebenso geeignete Massnahmen getroffen werden, um die Sicherheit ihrer eigenen Informationssysteme und Geräte zu gewährleisten.

1.1 SICHERER UMGANG MIT DATEN UND ARBEITSGERÄTEN

Es muss darauf geachtet werden, dass Daten und Informationen geheim gehalten und niemals an Dritte weitergegeben oder zugänglich gemacht werden.

- Sicherstellen, dass beim Verlassen des Arbeitsplatzes/-ortes immer alle Dokumente so versorgt und verschlossen sind, dass diese nicht für andere Personen zugänglich sind
- Sensible Dokumente entsprechend entsorgen, wie beispielsweise durch Schreddern
- Arbeitsgeräte, insbesondere Smartphone, Tablet und Laptop über ein sicheres Passwort schützen, welches niemandem sonst bekannt ist
- Darauf achten, dass der Computer beim Verlassen des Arbeitsplatzes gesperrt ist
- Keine Ausdrücke unbeaufsichtigt im Drucker/ Kopierer oder an anderen Stellen liegen lassen
- Dem IT-Verantwortlichen jede mutmassliche Verletzung oder versuchte Verletzung eines Kontos und generell jede Fehlfunktion im Zusammenhang mit einer Authentifizierung melden
- Den Authentifikator oder das persönliche Passwort in keiner Weise, auch nicht vorübergehend, an Dritte weitergeben oder übertragen

In den Applikationen von Circet Switzerland sind teilweise sensible Daten oder Kundeninformationen gespeichert bzw. dokumentiert. In diesem Zusammenhang ist die höchste Sicherheit und Sorgfalt geboten. Unter keinen Umständen dürfen solche Informationen an Dritte gelangen.

1.2 PHISHING

Es heisst besonders wachsam zu sein, wenn man seltsame oder fragwürdige Nachrichten von unbekannten Absendern erhält, welche Links zu unerwünschten Websites und/ oder Anhängen enthält oder zu ungewöhnlichen Handlungen auffordert. Bestehen bei einer Nachricht Zweifel an der Herkunft oder dem Inhalt, sind die zugehörigen Anhänge oder Hyperlinks NICHT zu öffnen. Jegliche Form von Phishing muss unverzüglich an den IT-Verantwortlichen gemeldet werden.

1.3 SPEICHERN VON DATEN

Es dürfen keine internen Daten im «normalen» Dateisystem der IT-Geräte abgespeichert werden. Es muss dafür immer die von Circet Switzerland zur Verfügung gestellte Applikation benutzt werden. Das Speichern auf portablen Datenträgern wie USB-Sticks ist verboten. Das Abspeichern von Informationen und Dateien auf privaten oder externen Geräten ist untersagt.

1.4 MOBILE DEVICES (SMARTPHONES & TABLETS)

Mobile Devices, wie Smartphones und Tablets, sind wichtige Tools für die Organisation des täglichen Arbeitseinsatzes. Dadurch gibt es gewisse Risiken, dass diese beispielsweise in falsche Hände geraten und sich dadurch Dritte Zugang zu unseren Daten und unserem IT-System verschaffen können. Daher sind alle Mobile Devices zwingend mit einem Passwort zu versehen (vgl. Ziffer 1.5).

1.5 PASSWÖRTER

Um den Schutz der Daten zu gewährleisten, muss auf jedem Smartphone und Tablet ein sicheres Passwort gesetzt werden. Dieses soll aus mindestens sechs Ziffern bestehen. Es muss darauf geachtet werden, dass dieses Passwort nicht für private Geräte eingesetzt wird. Ziel ist es, dass eine möglichst hohe Sicherheit bei Verlust oder Unachtsamkeit gegeben ist.

1.6 DOWNLOADS

Auf den von Circet Switzerland zur Verfügung gestellten Geräten dürfen keine fremden Softwares oder illegalen Inhalte geladen werden. Anwendungen dürfen nur aus offiziellen Plattformbetreibern installiert werden. Die Installation von Applikationen aus nicht vertrauenswürdigen Quellen ist untersagt. Dies wird auch für die IT-Geräte der Subunternehmen und Lieferanten empfohlen.

1.7 VORGEHEN BEI VERLUST UND/ ODER DIEBSTAHL

Liegt die Annahme für einen Diebstahl oder Verlust eines Gerätes vor, ist der entsprechende Systemadministrator von Circet Switzerland unmittelbar in Kenntnis zu setzen. Zudem wird diese Ansprechperson auch dann unverzüglich informiert, falls man den Verdacht hat, dass die Daten nicht genügend geschützt sind oder ein fremder Zugang vermutet wird. In einem solchen Fall kann diese Person den Zugriff respektive den fremden User sperren.

2. DATENSCHUTZ

Die Subunternehmer und Lieferanten von Circet Switzerland verpflichten sich dazu, das totalrevidierte Datenschutzgesetz (DSG) vom 1. September 2023 und die Ausführungsbestimmungen in der neuen Datenschutzverordnung sowie die neue Verordnung über Datenschutzzertifizierungen (VDSZ) und die damit verbundenen Anweisungen strikt einzuhalten.

2.1 PFLICHTEN BEI DER DATENBEARBEITUNG

Diese Pflichten an den Subunternehmer sollen ein hohes Mass an Datenschutz und -sicherheit gewährleisten und die Rechte der Personen, deren Daten verarbeitet werden, schützen:

Datenbearbeitung

Der Subunternehmer verpflichtet sich, Daten (insbesondere Kunden- und Personendaten) und Bearbeitungsergebnisse nur im Rahmen der Weisungen von Circet Switzerland zu verarbeiten und insbesondere nicht zu eigenen Zwecken.

Sicherheitsmassnahmen

Der Subunternehmer gestaltet seine Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle dem Risiko angemessenen technischen und organisatorischen Massnahmen, um die Vertraulichkeit, Verfügbarkeit und Integrität der Daten, die Nachvollziehbarkeit der Bearbeitung sicherzustellen und beachtet dabei zumindest die festgehaltenen IT-Sicherheitsmassnahmen. Er weist diese Massnahmen und deren Umsetzung auf Anfrage gegenüber Circet Switzerland nach.

Unterstützungspflichten

Der Subunternehmer unterstützt Circet Switzerland bei der Einhaltung der gesetzlichen Pflichten hinsichtlich des Datenschutzes (z.B. Datensicherheitsmassnahmen, Meldungen von Verletzungen an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung betroffenen Person). Der Subunternehmer meldet umgehend an Circet Switzerland alle ihm bekannt gewordenen Verstösse gegen Vorschriften oder Weisungen hinsichtlich der Personen- und/ oder Kundendaten und trifft alle erforderlichen Massnahmen zur Sicherung und Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

Betroffenenrechte

Der Subunternehmer ergreift die technischen und organisatorischen Massnahmen, damit Circet Switzerland die Rechte der betroffenen Person gemäss den anwendbaren Datenschutzgesetzen insbesondere aber Information, Auskunft, Berichtigung und Löschung (bzw. Anonymisierung), Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindungen im Einzelfall innert der gesetzlichen Frist erfüllen kann und überlässt Circet Switzerland alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Subunternehmer gerichtet, wird er den Antrag unverzüglich an Circet Switzerland zur Bearbeitung weiterleiten.

Löschungs- und Herausgabepflicht

Der Subunternehmer berichtigt, löscht (bzw. anonymisiert) oder sperrt Kundendaten nur auf Anweisung von Circet Switzerland und stellt dabei datenschutzkonforme Prozesse sicher. Vorbehalten bleiben Auskunfts- und Herausgabepflichten. Bei Vertragsende oder auf Verlangen von Circet Switzerland hat der Subunternehmer, einzelne oder alle Bearbeitungsergebnisse und Unterlagen, die Kundendaten enthalten, an Circet Switzerland zu übergeben oder nach Absprache in dessen Auftrag zu vernichten.

Ort der Datenverarbeitung

Der Subunternehmer und die von ihm beigezogenen Dritten dürfen die Daten nur in der Schweiz, einem Mitgliedsstaat der Europäischen Union (EU) oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) verarbeiten. Jede Datenbearbeitung ausserhalb der Schweiz, der EU oder des EWR bedarf der vorherigen schriftlichen Zustimmung von Circet Switzerland.

2.2 DATENSCHUTZBEAUFTRAGTE CIRCET SWITZERLAND

Die Datenschutzbeauftragte von Circet Switzerland ist Olivia Ursprung. E-Mail: olivia.ursprung@circet.ch
Der Subunternehmer meldet alle ihm bekannt gewordenen Verstösse gegen Vorschriften oder Weisungen hinsichtlich der Personen- und/ oder Kundendaten unverzüglich an die Datenschutzbeauftragte von Circet Switzerland.

2.3 INFORMATIONSPFLICHTEN UND AUDITRECHTE

Der Subunternehmer informiert Circet Switzerland umfassend über alle Umstände, welche die Leistungserbringung gefährden. Bei sicherheits- und datenschutzrelevanten Vorfällen informiert er Circet Switzerland schriftlich so rasch wie möglich, aber spätestens innerhalb von 72 Stunden, seit der Subunternehmer in ausreichendem Umfang von einem Vorfall Kenntnis erhalten hat. Erst später gewonnene Erkenntnisse liefert er umgehend nach. Es liegt anschliessend in der Verantwortung von Circet Switzerland erforderliche Anzeigen an Datenschutz- oder Aufsichtsbehörden zu veranlassen. Er informiert den Subunternehmer transparent über das geplante Vorgehen.

Der Subunternehmer weist die Einhaltung der Datenschutzvorschriften mit geeigneten Mitteln nach und erteilt Circet Switzerland auf Anfrage alle erforderlichen Auskünfte.

2.4 DATENSCHUTZVERLETZUNG UND HAFTUNG

Bei einer Datenschutzverletzung ist in jedem Fall die Datenschutzbeauftragte von Circet Switzerland zu informieren, welche eine Meldung an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) macht sowie die weiteren Schritte prüft. Der Subunternehmer und Circet Switzerland haften für den Schaden, der durch eine nicht gesetzes- oder vereinbarungskonforme Bearbeitung verursacht wird im Aussenverhältnis gemeinsam gegenüber der betroffenen Person.

Soweit Circet Switzerland zum Schadenersatz gegenüber der betroffenen Person verpflichtet ist, bleibt ihm der Rückgriff auf den Subunternehmer vorbehalten. Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben vorbehalten.

3. ABSCHLUSS

Bei einem Verstoss der Richtlinien oder missbräuchlichem Umgang mit den IT-Arbeitsgeräten oder Datenbearbeitung behält sich Circet Switzerland vor, bei den Subunternehmen eine Verwarnung oder bei schwerwiegenden Fällen, eine Vertragskündigung auszusprechen.