Talus Informatik AG
Verkauf & Marketing

Stückirain 10
3266 Wiler bei Seedorf
+41 32 391 90 90
servicedesk@talus.ch
www.talus.ch

Privacy Statement

Stand 29.11.2024

Inhalt

1 Vertragszweck 3

2 Zweckbindung der Datenbearbeitung 3

3 Vertraulichkeit 3

4 Einhaltung von Datenschutzgrundsätzen 3

5 Zertifizierung / Normen 4

6 Datenschutzverantwortliche; Verzeichnis der Bearbeitungstätigkeiten 4

7 Datensicherheit 4

8 Umgang mit vertraulichen Daten / Sicherstellung der Datensicherheit 6

9 Subunternehmer / Angestellte 6

10 Bearbeitung im Ausland 6

11 Archivierung und Vernichtung 7

12 Umsetzung der Rechte der betroffenen Personen 7

13 Vorgehen bei Verletzungen des Datenschutzes 7

14 Dauer 8

15 Abänderung der Vereinbarung / Unwirksamkeit von Bestimmungen 8

16 Gerichtsstand / anwendbares Recht 8

1 Vertragszweck

Die Talus Informatik AG (nachfolgend «Talus») erbringt basierend auf dem «Rahmenvertrag über IT-Dienstleistungen» und seinen Anhängen und Begleitdokumenten oder aufgrund eines sonstigen separaten Vertrags mit dem KUNDEN (nachfolgend: «der Hauptvertrag») Leistungen im Bereich IT-Lösungen und IT-Support für den KUNDEN. Zu diesem Zweck bearbeitet Talus als Auftragsbearbeiterin vom KUNDEN zugänglich gemachte Personendaten natürlicher Personen (nachfolgend: die «Personendaten»). Dieses Privacy Statement stellt als Zusatzvereinbarung zum Hauptvertrag die Einhaltung des Datenschutzgesetzes im Rahmen dieser Auftragsdatenbearbeitung sicher. Es findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag im Zusammenhang stehen und bei denen Talus die Personendaten bearbeitet.

Diese Zusatzvereinbarung ergänzt den Hauptvertrag. Im Falle von Widersprüchen gehen die datenschutzspezifischen Bestimmungen des Hauptvertrags oder schriftlich festgehaltene Abmachungen im Einzelfall den Bestimmungen des Privacy Statements vor. Datenschutzspezifische Bestimmungen dieses Zusatzvertrags gehen dagegen allgemein gefassten (nicht datenschutzspezifischen) Regelungen des Hauptvertrags vor.

2 Zweckbindung der Datenbearbeitung

Talus verpflichtet sich, die Personendaten nur zwecks Erfüllung ihrer vertraglichen Verpflichtungen aus dem Hauptvertrag zu bearbeiten. Eine Verwendung zu anderen Zwecken ist nicht erlaubt.

Der KUNDE ist für die rechtmässige Weitergabe der Personendaten an Talus verantwortlich und ist hinsichtlich der Bearbeitung durch Talus weisungsbefugt. Er stellt wo nötig durch einschränkende Weisungen gegenüber Talus sicher, dass die Personendaten von Talus nur in dem Umfang bearbeitet werden, wie er es gemäss den für ihn geltenden kantonalen oder eidgenössischen Gesetzesvorgaben selber tun dürfe. Er sichert Talus in diesem Zusammenhang zu, dass der Bearbeitung der Personendaten durch Talus zum Zweck der Erfüllung des Hauptvertrags keine rechtlichen Hindernisse entgegenstehen oder er Talus sonst auf entsprechende Einschränkungen aufmerksam gemacht hat.

3 Vertraulichkeit

Talus hält die Personendaten soweit diese nicht bereits nachweislich öffentlich bekannt sind vertraulich und sieht soweit der Hauptvertrag oder dieser Vertragszusatz keine Ausnahmen vorsehen von der Weitergabe an Dritte ab.

4 Einhaltung von Datenschutzgrundsätzen

Bei der Bearbeitung der Personendaten hält Talus die folgenden datenschutzrechtlichen Grundsätze ein:

- Rechtmässige Datenbeschaffung
- Bearbeitung nach Treu und Glauben und der Verhältnismässigkeit
- Vernichtung oder Anonymisierung der Daten wenn sie zum vorgesehenen Zweck nicht
- mehr gebraucht werden und keine gesetzlichen Aufbewahrungspflichten entgegenstehen
- Daten müssen wahrheitsgetreu sein
- Daten müssen durch angemessene technische und organisatorische Massnahmen ge
- gen unbefugtes Bearbeiten geschützt sein.
- Die Daten sind nach den Grundsätzen «Privacy bei Design» (Datenschutz durch Technik)
- und «Privacy bei Default» (Datenschutz durch datenschutzfreundliche Voreinstellungen) zu bearbeiten.

5 Zertifizierung / Normen

Talus ist seit Dezember 2004 mit dem Datenschutzlabel «GoodPriv@cy®» zertifiziert. Datenschutzgütesiegel: Zertifizierung von Organisationen, die Personendaten bearbeiten (siehe auch http://www.sqs.ch). Im Bereich Informationssicherheit richtet sich die Tätigkeit von Talus nach den ISO Normen 27001 und 27002.

6 Datenschutzverantwortliche; Verzeichnis der Bearbeitungstätigkeiten

Talus verpflichtet sich eine Person zu bestimmen, welche als Datenschutzverantwortliche für die Einhaltung der datenschutzrechtlichen Bestimmungen sowie die Beantwortung datenschutzrechtlicher Anfragen des Kunden verantwortlich ist. Der Kunde kann die Datenschutzverantwortliche schriftlich über folgende Emailadresse kontaktieren:

Email: servicedesk@talus.ch

Ein Verzeichnis der Bearbeitungstätigkeiten ist zu erstellen sofern Talus für den KUNDEN umfangreiche Bearbeitungen besonders schützenswerter Personendaten vornimmt oder Personendaten verknüpft, um Persönlichkeitsprofile zu erstellen, welche ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen.

Ist der KUNDE selber verpflichtet, ein Verzeichnis der Bearbeitungstätigkeiten über die Personendaten zu führen und/oder ist er der Ansicht, dass Talus als Auftragsbearbeiter dazu verpflichtet ist, so teilt er dies Talus mit und stellt ihr falls vorhanden soweit die von Talus vorzunehmenden Bearbeitungsvorgänge betreffend Auszüge aus dem von ihm geführten Bearbeitungsverzeichnis zur Verfügung.

Das von Talus zu erstellende Verzeichnis wird schriftlich von der Datenschutzverantwortlichen geführt und regelmässig aktualisiert. Es gibt Aufschluss über:

- Den für die Bearbeitung verantwortlichen KUNDEN
- Die Rolle der Talus als Auftragsbearbeiterin
- Die Kategorien der Bearbeitungen, die im Auftrag des KUNDEN durchgeführt werden
- Einen allgemeinen Beschrieb der Massnahmen zur Gewährleistung der Datensicherheit
- Falls die Daten ins Ausland bekanntgegeben werden die Angabe der Staaten sowie der
- Garantien bezüglich Einhaltung des Datenschutzes

7 Datensicherheit

Zur Gewährleistung einer angemessenen Datensicherheit legt Talus aufgrund der vom KUNDEN stammenden Informationen über den Schutzbedarf der Personendaten die im Hinblick auf das Risiko geeigneten technischen und organisatorischen Massnahmen zur Sicherstellung der Datensicherheit fest.

Der Schutzbedarf der Personendaten (hoher, mittlerer oder tiefer Schutzbedarf) wird Talus vom KUNDEN mittels des Formulars «Schutzbedarf von Personendaten» mitgeteilt und bestimmt sich nach den Kriterien Art der Daten, Zweck, Art, Umfang und Umstände der Bearbeitung. Das Risiko für die betroffenen Personen wird von Talus sodann nach den Kriterien Ursachen des Risikos, hauptsächliche Gefahren, ergriffene oder vorgesehene Risikoverminderungsmassnahmen sowie Wahrscheinlichkeit und Schwere einer Datensicherheitsverletzung trotz der ergriffenen oder vorgesehenen Massnahmen beurteilt. Bei der Festlegung der Massnahmen sind der Stand der Technik sowie die Implementierungskosten zu berücksichtigen. Das resultierende Datensicherheitsdispositiv ist regelmässig zu überprüfen und wo erforderlich anzupassen.

Um die Datensicherheit sicherzustellen, trifft Talus technische und organisatorischen Massnahmen, damit die in ihrem Herrschaftsbereich bearbeiteten Personendaten.

- nur Berechtigten zugänglich sind (Vertraulichkeit);
- verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);
- nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);
- nachvollziehbar bearbeitet werden (Nachvollziehbarkeit)

Um die Vertraulichkeit zu gewährleisten, trifft Talus geeignete Massnahmen, damit:

- berechtigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle);
- nur berechtigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden (Zugangskontrolle);
- unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können (Benutzerkontrolle).

Um die Verfügbarkeit und Integrität zu gewährleisten, trifft Talus geeignete Massnahmen damit:

- unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können (Datenträgerkontrolle);
- unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können (Speicherkontrolle);
- unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können (Transportkontrolle);
- die Verfügbarkeit der Personendaten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (Wiederherstellung);
- alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität);
- Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (Systemsicherheit).

Um die Nachvollziehbarkeit zu gewährleisten, trifft Talus geeignete Massnahmen damit:

- überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher
- Person eingegeben oder verändert werden (Eingabekontrolle);
- überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur Datenüber-
- tragung bekanntgegeben werden (Bekanntgabekontrolle);
- Verletzungen der Datensicherheit rasch erkannt (Erkennung) und Massnahmen zur Min-
- derung oder Beseitigung der Folgen ergriffen werden können (Beseitigung).

Eine Zusammenstellung der von Talus für ihre IT-Systeme, auf denen die Personendaten bearbeitet werden, getroffenen technischen und organisatorischen Massnahmen findet sich im separaten Informationsblatt «Technische und Organisatorische Massnahmen (TOM)». Der KUNDE ist befugt, von Talus weiteren Aufschluss über die konkret getroffenen technischen und organisatorischen Massnahmen zur Einhaltung des Datenschutzes für die Personendaten zu verlangen.

Erbringt Talus Leistungen im Herrschaftsbereich des KUNDEN, d.h. vor Ort beim KUNDEN oder durch Fernzugriff auf IT-Systeme von KUNDEN (z.B. Support-Leistungen), bei denen die Personendaten zugänglich gemacht werden, so ist der KUNDE in seinem Herrschaftsbereich für

die Sicherstellung der technischen und organisatorischen Massnahmen zur Sicherstellung des Datenschutzes verantwortlich und teilt Talus die entsprechenden Vorgaben mit.

8 Umgang mit vertraulichen Daten / Sicherstellung der Datensicherheit

Talus stellt einen angemessenen, professionell betreuten, dem Stand der Technik entsprechenden und laufend aktualisierten Schutz (Antivirus, Firewall, Antispyware, Backup) ihrer IT-Systeme, auf denen die Personendaten bearbeitet werden, sicher.

Emails oder sonstige elektronische Nachrichten mit vertraulichen Personendaten sind grundsätzlich verschlüsselt bzw. via verschlüsselte Verbindungen zu verschicken. Datenträger mit vertraulichen Personendaten sind nur in verschlüsselter Form an externe Stellen oder Personen zu verschicken.

In elektronischer Form vorhandene vertrauliche Daten sind passwortgeschützt zu verwahren.

Vertrauliche Personendaten dürfen weder elektronisch noch physisch für Dritte einsehbar sein.

Dokumente/Akten in Papierform und mobile Speichermedien mit vertraulichen Daten sind von Mitarbeitern von Talus bei Verlassen des Arbeitsplatzes aus dem Sichtbereich zu entfernen. Mit geeigneten Zutrittsschranken ist sicherzustellen, dass unbefugte Dritte am Zugang zu Gebäuden oder Gebäudeteilen, in denen vertrauliche Personendaten bearbeitet werden, gehindert werden.

9 Subunternehmer / Angestellte

Talus ist befugt, die Personendaten durch Subunternehmer bearbeiten zu lassen, sofern diese vertraglich in gleichwertiger Weise zur Wahrung des Datenschutzes verpflichtet sind wie Talus.

Auf Verlangen gibt Talus dem KUNDEN die für die Datenbearbeitung beigezogenen Subunternehmer sowie den Umfang der Datenbearbeitung durch diese Subunternehmer bekannt. Sie informiert den KUNDEN über beabsichtigte Änderungen in Bezug auf Subunternehmer. Der KUNDE ist berechtigt, solche Änderungen abzulehnen, sofern durch die Änderung die Einhaltung eines gleichwertigen Datenschutzes aus nachvollziehbaren Gründen ernsthaft in Frage gestellt wird.

Talus stellt sicher, dass Angestellte, welche die Personendaten bearbeiten, arbeitsvertraglich zur Einhaltung des Datenschutzes und insbesondere der Vertraulichkeit in Bezug auf die Personendaten verpflichtet sind.

10 Bearbeitung im Ausland

Je nach den vom KUNDEN bezogenen Produkten lässt Talus Personendaten durch

Subunternehmer im Ausland bearbeiten, wozu auch die Speicherung auf ausländischen IT-Systemen (z.B. «Cloud», mit Servern im Ausland) gehört. Die Datenbearbeitung findet dabei soweit nicht ausdrücklich anders angegeben ausschliesslich durch vertraglich zur Einhaltung des Datenschutzes und der Vertraulichkeit verpflichtete Subunternehmer in EU-Ländern statt und ist der EU-Datenschutzgesetzgebung (EU-DSGVO) unterstellt.

Die betroffenen Produkte/Länder sind im separaten Informationsblatt «Datenbearbeitung im Ausland» ersichtlich. Dieses wird von Talus laufend aktualisiert, wobei dem KUNDEN

Aktualisierungen jeweils mitzuteilen sind. Der KUNDE ist befugt, von Talus weiteren Aufschluss über die Bearbeitung der Personendaten im Ausland zu verlangen.

Es ist Sache des KUNDEN, sicherzustellen, dass die von Talus bekanntgegebene Bearbeitung von Personendaten im Ausland aus Sicht Datenschutz und allfälliger anderer gesetzlicher oder vertraglicher Vorgaben zulässig ist.

11 Archivierung und Vernichtung

Die bei Talus verbleibende Personendaten sind von Talus nach Abschluss der Vertragstätigkeit innert angemessener Frist in Absprache mit dem KUNDEN zu vernichten bzw. zu löschen oder ohne Rückbehalt von Kopien an den KUNDEN zu übergeben. Dort wo Talus gesetzlich verpflichtet ist, die Personendaten als Belege ihrer Tätigkeit aufzubewahren, sind sie spätestens nach Ablauf der gesetzlichen Aufbewahrungsfrist, in der Regel nach 10 Jahren, zu vernichten. Dort wo Talus gemäss Hauptvertrag zu einer längeren Aufbewahrung verpflichtet ist (Archivdienste, etc.), sind sie gemäss den vertraglichen Vorgaben aufzubewahren und danach in Absprache mit dem KUNDEN zu vernichten bzw. zu löschen oder ohne Rückbehalt von Kopien an den KUNDEN zu übergeben

Die fachgerechte Entsorgung von digitalen Datenträgern, welche vertrauliche Personendaten enthalten bzw. von Hardware, welche solche Datenträger enthält, ist durch einen geeigneten professionellen, der Vertraulichkeit verpflichteten Anbieter zu veranlassen, welcher die irreversible Vernichtung der Daten sicherstellt.

Die Entsorgung vertraulicher Personendaten in nicht-digitaler Form, so insbesondere in Papierform, hat via Schredder oder über besonders markiert Behältnisse zu erfolgen, bei denen anschliessend eine Vernichtung durch ein spezialisiertes, der Vertraulichkeit verpflichtetes Abfuhrunternehmen erfolgt. Vertrauliche Personendaten sind nicht im allgemeinen Abfall zu entsorgen.

12 Umsetzung der Rechte der betroffenen Personen

Talus ist verpflichtet, den KUNDEN bei der Umsetzung der sich aus dem DSG ergebenden Rechte der von der Bearbeitung der Personendaten betroffenen Personen wie etwa Rechte auf Auskunft, Herausgabe, Löschung, Sperrung, Korrektur, Widerruf von Einwilligungen, etc. zu unterstützen. Es ist dabei Sache des KUNDEN, entsprechende Ersuchen der betroffenen Personen entgegenzunehmen, zu beurteilen und ggfls. mit Unterstützung durch Talus umzusetzen. Talus ist nicht berechtigt, ohne entsprechende Absprache mit dem KUNDEN von sich aus entsprechende Ersuchen von Betroffenen entgegenzunehmen und umzusetzen. Sofern seitens Talus überwiegende Interessen oder gesetzliche Vorgaben entgegenstehen, ist sie berechtigt, die Unterstützung bei der Umsetzung der Betroffenenrechte zu verweigern.

13 Vorgehen bei Verletzungen des Datenschutzes

Im Falle einer Datenschutzverletzung, insbesondere der Preisgabe von vertraulichen Personendaten an Unbefugte, sowie des Verlustes oder der Veränderung der Personendaten, der drohenden Gefahr einer solchen Verletzung oder des konkreten Verdachtes auf eine solche Verletzung ist der KUNDE unverzüglich zu informieren. Die von ihm in der Folge erteilten

Weisungen sind von Talus strikt zu befolgen. Der KUNDE entscheidet, welche Massnahmen zu treffen sind und ob eine Meldung an die Behörden sowie eine Information betroffener Personen erforderlich ist.

14 Dauer

Die Pflicht zur Einhaltung des Datenschutzes gilt auch nach Beendigung des Hauptvertrags weiter, solange Talus Zugang zu den Personendaten hat.

15 Abänderung der Vereinbarung / Unwirksamkeit von Bestimmungen

Ergänzungen oder Abänderungen dieser Vereinbarung bedürfen zu ihrer Gültigkeit der Schriftform. Sollte eine Bestimmung in dieser Vereinbarung unwirksam sein oder werden, so gilt an deren Stelle eine wirksame Bestimmung als vereinbart, die dem von den Parteien gewollten Ergebnis wirtschaftlich am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.

16 Gerichtsstand / anwendbares Recht

Es gelten die entsprechenden Bestimmungen des Hauptvertrags. Sofern nicht im Hauptvertrag geregelt ist allein materielles Schweizer Recht anwendbar, mit ausschliesslichem Gerichtsstand in Wiler bei Seedorf.