Talus Informatik AG
Verkauf & Marketing

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

Datenschutz

Infoblatt technische und organisatorische Massnahmen (TOM)

Inhaltsverzeichnis

Zwecks Wahrung der Datensicherheit in Bezug auf Personendaten ihrer Kunden trifft die Talus Informatik AG (nachfolgend «Talus») die folgen-den technischen und organisatorischen Massnahmen:

1 Zertifizierung

Talus ist seit Dezember 2004 mit dem Datenschutzlabel «GoodPriv@cy®» zertifiziert. Datenschutzgütesiegel: Zertifizierung von Organisationen, die Personendaten bearbeiten (siehe auch http://www.sqs.ch)

2 Physische Zugangskontrolle

Unbefugten wird der physische Zugang zu Grundstücken, Gebäuden oder Räumen verwehrt, in denen sich Datenbearbeitungssysteme befinden, die Personendaten verarbeiten und/oder nutzen.

Massnahmen

- Talus schützt ihre Anlagen und Einrichtungen mit den geeigneten Mitteln auf der Grundlage einer intern durchgeführten Sicherheitsklassifizierung.
- Im Allgemeinen sind die Gebäude durch Zugangskontrollsysteme gesichert.
- Die äussersten Zugänge der Gebäude sind mit einem zertifizierten Schlüsselsystem mit modernem, aktivem Schlüsselmanagement ausgestattet.
- Je nach Sicherheitseinstufung können Gebäude, einzelne Bereiche und das umliegende Gelände durch zusätzliche Massnahmen weiter geschützt werden.
- Die Zutrittsrechte werden den berechtigten Personen entsprechend den Massnahmen zur System- und Datenzugangskontrolle auf individueller Basis gewährt. Dies gilt auch für den Zutritt von Besuchern. Gäste und Besucher der Talus-Gebäude müssen sich an der Rezeption namentlich registrieren lassen und müssen von autorisiertem Talus-Personal begleitet werden.

Zusätzliche Massnahmen für Rechenzentren

- Alle Rechenzentren unterliegen strengen Sicherheitsvorkehrungen, die durch Wachpersonal, Überwachungskameras, Bewegungsmelder, Zugangskontrollmechanismen und andere Massnahmen durchgesetzt werden, um zu verhindern, dass Geräte und Einrichtungen des Rechenzentrums für unbefugte Personen zugänglich sind oder gestört werden können. Nur befugte Vertreter haben Zugang zu den Systemen und der Infrastruktur in den Einrichtungen des Rechenzentrums. Um die ordnungsgemässe Funktionalität zu gewährleisten, wird die physische Sicherheitsausrüstung (z.B. Bewegungsmelder, Kameras usw.) regelmässig gewartet.
- Talus und alle Drittanbieter von Rechenzentren protokollieren die Namen und Zeiten der Personen, die die privaten Bereiche der Rechenzentren von Talus betreten.

3 Systemzugangskontrolle

Die zur Erbringung der Talus Dienstleistungen eingesetzten Datenbearbeitungssysteme sind vor unbefugter Nutzung zu schützen.

Massnahmen

- Bei der Gewährung des Zugangs zu sensiblen Systemen, einschliesslich solcher, die Personendaten speichern und bearbeiten, werden mehrere Berechtigungsstufen verwendet. Es gibt Verfahren, die sicherstellen, dass autorisierte Benutzer über die entsprechende Berechtigung zum Hinzufügen, Löschen oder Ändern von Benutzern verfügen.
- Alle Benutzer haben mit einer eindeutigen Kennung (Benutzer-ID) Zugang zu den Systemen der Talus.

- Beim Betrieb des Rechenzentrums und bei kritischen Systemen wird eine Zwei-Faktor-Authentifizierung durchgesetzt.
- Talus verfügt über Vorgaben und Verfahren, die sicherstellen, dass beantragte Berechtigungsänderungen nur in kontrollierter Weise durchgeführt werden (z.B. werden keine Rechte ohne Kontrolle der Berechtigung vergeben). Verlässt ein Benutzer das Unternehmen, werden ihm die Zugriffsrechte entzogen.
- Talus hat eine Passwort-Policy aufgestellt, die die Weitergabe von Passwörtern verbietet, die Reaktionen auf die Offenlegung von Passwörtern regelt und die regelmässige Änderung von Passwörtern sowie die Änderung von Standardpasswörtern vorschreibt. Zur Authentifizierung werden personalisierte Benutzer-IDs vergeben. Alle Passwörter müssen definierten Mindestanforderungen genügen und werden verschlüsselt gespeichert. Bei Domänenpasswörtern erzwingt das System alle sechs Monate eine Passwortänderung, um die Anforderungen an komplexe Passwörter zu erfüllen. Jeder Computer verfügt über einen passwortgeschützten Bildschirmschoner.
- Das Unternehmensnetz ist durch Firewalls vom öffentlichen Netz abgeschirmt.
- Es wird ein Sicherheits-Patch-Management eingeführt, um eine regelmässige und periodische Verteilung der relevanten Sicherheits-Updates zu gewährleisten.
- Der vollständige Fernzugriff auf das Unternehmensnetz und die kritische Infrastruktur von Talus ist durch eine starke Authentifizierung geschützt.

4 Datenzugangskontrolle

Personen, die berechtigt sind, Datenbearbeitungssysteme zu nutzen, erhalten nur Zugang zu den Personendaten, auf die sie ein Zugriffsrecht haben, und Personendaten dürfen im Verlauf der Bearbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Massnahmen

- Im Rahmen der Talus Sicherheitsvorgaben müssen Personendaten grundsätzlich vertraulich gehalten werden.
- Der Zugang zu persönlichen, vertraulichen oder sensiblen Informationen wird nach dem «Need-to-know-Prinzip» gewährt. Mit anderen Worten: Mitarbeiter oder externe Dritte haben nur Zugang zu den Informationen, die sie für ihre Arbeit benötigen. Talus verwendet Authorisierungskonzepte, die dokumentieren, wie Berechtigungen vergeben werden und welche Berechtigungen an wen vergeben werden. Alle personenbezogenen, vertraulichen oder anderweitig sensiblen Daten werden gemäss den Talus-Sicherheitsrichtlinien und -Standards geschützt. Vertrauliche Informationen müssen vertraulich verarbeitet werden.
- Alle Produktionsserver werden in den Data Centern oder in sicheren Serverräumen betrieben. Die Sicherheitsmassnahmen zum Schutz von Anwendungen, die Personendaten verarbeiten, werden regelmässig überprüft. Zu diesem Zweck führt Talus interne und externe Sicherheitsüberprüfungen und Penetrationstests ihrer IT-Systeme durch.
- Talus erlaubt nicht die Installation von persönlicher Software oder anderer Software, die nicht von Talus genehmigt wurde.
- Interne Sicherheitsvorgaben regeln, wie Daten und Datenträger gelöscht oder gelöscht werden.

5 Kontrolle der Datenübertragung

Personendaten dürfen während der Übermittlung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Werden Datenträger physisch transportiert, so werden bei Talus geeignete Massnahmen getroffen, um die vereinbarten Schutzstufen zu gewährleisten (z.B. Verschlüsselung).

Massnahmen

- Personendaten, die über Talus-interne Netze übertragen werden, sind in der gleichen Weise geschützt wie alle anderen vertraulichen Daten.
- Bei Datenübertragungen zwischen Talus und ihren Kunden werden die Schutzmassnahmen für die übertragenen Personendaten einvernehmlich festgelegt und zum Bestandteil der jeweiligen Vereinbarung gemacht. Dies gilt sowohl für die physische als auch für die netzbasierte Datenübertragung. In jedem Fall übernimmt der Kunde die Verantwortung für den Datentransfer, sobald er sich ausserhalb der von Talus kontrollierten Systeme befindet (z.B. Daten, die ausserhalb der Firewall des Talus-Rechenzentrums übertragen werden).

6 Kontrolle der Dateneingabe

Es kann nachträglich überprüft und festgestellt werden, ob und von wem Personendaten in die Talus Datenbearbeitungssysteme eingegeben, verändert oder entfernt wurden.

Massnahmen

- Talus erlaubt nur befugten Personen den Zugriff auf Personendaten, soweit dies im Rahmen ihrer Tätigkeit erforderlich ist.
- Talus hat ein Protokollierungssystem für die Eingabe, Änderung und Löschung oder Sperrung personenbezogener Daten durch Talus oder ihre Unterauftragsbearbeiter innerhalb der Produkte und Dienstleistungen von Talus so weit wie möglich implementiert.

7 Auftragskontrolle

Personendaten, die im Auftrag verarbeitet werden (d.h. Personendaten, die im Namen eines Kunden verarbeitet werden), werden ausschliesslich in Übereinstimmung mit dem entsprechenden Vertrag und den entsprechenden Anweisungen des Kunden verarbeitet.

Massnahmen

- Talus setzt Kontrollen und Prozesse ein, um die Einhaltung der Verträge zwischen Talus und ihren Kunden, Unterauftragnehmern oder anderen Dienstleistern sicherzustellen.
- Im Rahmen des Talus Sicherheitskonzepts müssen Personendaten mindestens das gleiche Schutzniveau wie sonstige "vertrauliche" Informationen aufweisen.
- Alle Talus Mitarbeiter und vertraglichen Unterauftragsbearbeiter oder andere Dienstleister sind vertraglich verpflichtet, die Vertraulichkeit aller sensiblen Informationen einschliesslich der Geschäftsgeheimnisse von Talus Kunden und Partnern zu respektieren.
- Für Supportleistungen vor Ort stellt Talus einen speziell ausgewiesenen, sicheren Support-Ticket-Bereich zur Verfügung, in dem Talus einen besonders zugangskontrollierten und überwachten Sicherheitsbereich für die Übertragung von Zugangsdaten und Passwörtern bereitstellt. Talus-Kunden haben jederzeit die Kontrolle über ihre Remote-Support-Verbindungen. Talus-Mitarbeiter können nicht ohne das Wissen oder die volle aktive Beteiligung des Kunden auf ein Kundensystem zugreifen.

8 Verfügbarkeitskontrolle

Persönliche Daten werden gegen zufällige oder unbefugte Zerstörung oder Verlust geschützt.

Massnahmen

- Talus setzt Backup-Prozesse und andere Massnahmen ein, die eine schnelle Wiederherstellung von geschäftskritischen Systemen im Bedarfsfall sicherstellen.
- Talus setzt unterbrechungsfreie Stromversorgungen (z.B. USV, Batterien, Generatoren, etc.) ein, um die Stromversorgung der Rechenzentren zu gewährleisten.

- Talus verfügt über definierte Notfallpläne sowie Business- und Disaster-Recovery-Strategien für die angebotenen Dienstleistungen.
- Die Notfallprozesse und -systeme werden regelmässig getestet.

9 Kontrolle der Datentrennung

Personendaten, die für unterschiedliche Zwecke erhoben werden, können getrennt verarbeitet werden.

Massnahmen

- Talus verwendet eine logische Trennung auf Repository-Ebene, um eine Datentrennung zwischen Personendaten zu erreichen, die von mehreren Kunden stammen.
- Talus verwendet getrennte Produktions- und Testumgebungen.
- Kunden (einschliesslich der mit ihnen verbundenen Unternehmen) haben nur Zugriff auf ihre eigenen Daten.
- Werden Personendaten für die Bearbeitung eines Supportfalls eines bestimmten Kunden benötigt, werden die Daten dieser bestimmten Nachricht zugeordnet und nur für die Bearbeitung dieser Nachricht verwendet; auf sie wird nicht für die Bearbeitung anderer Nachrichten zugegriffen. Diese Daten werden in speziellen Supportsystemen gespeichert.

10 Kontrolle der Datenintegrität

Personendaten bleiben während der Bearbeitung unversehrt, vollständig und aktuell.

Massnahmen

Talus hat eine mehrschichtige Abwehrstrategie zum Schutz vor unbefugten Änderungen implementiert.

Talus setzt insbesondere die folgenden Massnahmen ein, um die oben beschriebenen Kontroll- und Massnahmenbereiche umzusetzen. Im Einzelnen sind dies:

- Firewalls;
- Sicherheitsüberwachungszentrum;
- Backup und Wiederherstellung;
- Externe und interne Penetrationstests;
- Regelmässige externe Audits zum Nachweis der Sicherheitsmfassnahmen