RICHTLINIE ZUR DATENSICHERHEIT

Dieses Dokument (die "Richtlinie zur Datensicherheit") beschreibt die Sicherheitsanforderungen, die für alle Parteien einer Vereinbarung gelten, die mit der telXira GmbH oder einem mit ihr verbundenen Unternehmen (nachfolgend "telXira" genannt) unterzeichnet wurde. In besonderen Fällen können zusätzliche Sicherheitsanforderungen gelten, wenn diese von den beteiligten Parteien vereinbart wurden.

Definitionen

"**Vereinbarung**" bezeichnet die Vereinbarung zwischen telXira und seinem Geschäftspartner, unter der die Datensicherheitsrichtlinie Anwendung findet und für die die Datensicherheitsrichtlinie Teil dieser Richtlinie ist.

"**Käufer**" ist die Einheit, die Dienstleistungen von der anderen Partei bezieht und durch einen Dienstleistungsvertrag mit dieser anderen Partei, die als Lieferant definiert wird, gebunden ist.

"**Daten des Käufers**" sind Daten oder andere Informationen, die der Käufer oder eine im Namen des Käufers handelnde Person der anderen Partei zur Verfügung stellt, einschließlich, aber nicht beschränkt auf den Zweck der Verarbeitung personenbezogener Daten.

"Lieferant" bezieht sich auf die Gegenpartei, die dem Käufer jegliche Art von Liefergegenständen liefert, die in der betreffenden Vereinbarung als "Lieferant", "Anbieter, "Partner" oder gleichwertig gekennzeichnet sind.

"Personal des Lieferanten" ist jede Person, die im Auftrag des Lieferanten arbeitet, wie z.B. Mitarbeiter, Berater, Auftragnehmer und Unterlieferanten.

"**Informationsverarbeitungseinrichtungen**" sind alle Informationsverarbeitungssysteme, -dienste oder -infrastrukturen oder die physischen Orte, an denen sie untergebracht sind.

"**Protokoll**" ist die Aufzeichnung von Einzelheiten von Informationen oder Ereignissen in einem organisierten Aufzeichnungssystem, normalerweise in der Reihenfolge, in der die Informationen oder Ereignisse stattgefunden haben.

"**Personenbezogene Daten**" bezeichnet die gesamte Informationskommunikation (Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation) und die allgemeine Datenschutzverordnung (Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr), und zur Aufhebung der Richtlinie 94/46/RC) sowie deren Änderungen, Ersetzungen oder Erneuerungen (zusammen die "EU-Gesetzgebung"), alle verbindlichen nationalen Gesetze zur Umsetzung der EU-Gesetzgebung und anderer verbindlicher Richtlinien, Gesetze, Verordnungen und Urteile zum Datenschutz oder zur Datensicherheit, die zum gegebenen Zeitpunkt gültig sind und eine natürliche Person identifizieren. Eine identifizierbare natürliche Person ist eine Person, die direkt oder indirekt durch Bezugnahme auf einen Identifikator wie Name, Adresse, Sozialversicherungsnummer, Abonnementnummer, IP-Adresse, Standortdaten, einen Online-Identifikator, Verkehrsdaten oder Nachrichteninhalt oder auf einen oder mehrere Faktoren, die spezifisch für die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität dieser natürlichen Person sind, identifiziert werden kann.

"**Dienstleistungen**" sind die vom Lieferanten für den Käufer oder eine im Namen des Lieferanten handelnde Person zu erbringenden Dienstleistungen, wie in der Vereinbarung zwischen den Parteien näher definiert.

"**Sicherheitskontrolle**" ist eine technische Gegenmaßnahme, ein organisatorischer Aufbau oder ein Prozess, der dazu beiträgt, die Sicherheitseigenschaften von IT-Systemen zu erhalten.

"**Sicherheitszwischenfall**" bezeichnet ein einzelnes oder eine Reihe von unerwünschten oder unerwarteten Sicherheitsereignissen, die mit einer erheblichen Wahrscheinlichkeit den Geschäftsbetrieb gefährden und die Sicherheit bedrohen.

"**Sensible Produkte**" und "**Sensible Dienstleistungen**" sind alle Produkte oder Dienstleistungen, die vom Käufer als sensibel definiert werden. Sensible Produkte oder sensible Dienstleistungen müssen in der anwendbaren Vereinbarung klar dokumentiert werden.

"**Pseudonymisierung**" ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne die Verwendung zusätzlicher Informationen nicht mehr einer bestimmten Person zugeordnet werden können, vorausgesetzt, dass diese zusätzlichen Informationen getrennt aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die sicherstellen, dass die personenbezogenen Daten nicht einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden

Geltungsbereich

Die Richtlinie zur Datensicherheit gilt wann:

- Der Lieferant wird die Daten des Käufers verarbeiten;
- Der Lieferant wird auf das Netzwerk oder die IT-Systeme des Käufers zugreifen, einschließlich Fernzugriff;
- Der Lieferant kümmert sich um die Informationsverarbeitungsausrüstung des Käufers;
- der Käufer den Lieferanten als Anbieter von sensiblen Produkten und/oder sensiblen Dienstleistungen betrachtet und den Lieferanten als solchen im Rahmen der betreffenden Vereinbarung identifiziert hat.

Die Gesamtverantwortung des Lieferanten

Der Lieferant ist voll verantwortlich für die Einhaltung der Richtlinie zur Datensicherheit durch das Personal des Lieferanten.

Der Lieferant führt die erforderlichen Maßnahmen zur Gewährleistung der Einhaltung der Richtlinie zur Datensicherheit durch, bevor er einen Auftrag für den Käufer beginnt.

Auf Anfrage des Käufers informiert der Lieferant den Käufer darüber, wie der Lieferant die Richtlinie zur Datensicherheit einhält und welche Maßnahmen er zur Einhaltung der Richtlinie zur Datensicherheit ergriffen hat.

Der Lieferant informiert den Käufer so bald wie möglich, spätestens jedoch innerhalb von 24 Stunden nach Feststellung des Sicherheitsvorkommnisses (einschließlich, aber nicht beschränkt auf Vorfälle im Zusammenhang mit der Verarbeitung personenbezogener Daten) über jedes Sicherheitsvorkommnis. Siehe Vorfallmanagement weiter unten.

Der Lieferant garantiert, dass jegliche Verarbeitung der Daten des Käufers in Übereinstimmung mit der Richtlinie zur Datensicherheit erfolgt.

Der Lieferant muss alle Daten des Käufers und die Kopien davon zurückgeben oder vernichten (wie vom Käufer bestimmt). Der Lieferant muss dem Käufer bei Beendigung der Vereinbarung oder auf Verlangen des Käufers schriftlich bestätigen, dass der Lieferant diese Anforderung erfüllt hat.

Der Lieferant gewährt keiner Partei ohne vorherige schriftliche Zustimmung des Käufers Zugang zu den Daten des Käufers (es kann sich auch um neuen, erweiterten, aktualisierten, verlängerten oder

auf andere Weise geänderten Echtzeit-Netzwerkzugang handeln), die gegen die Vereinbarung verstoßen.

Sicherheitsanforderungen

Risiko-Management

1. Management von Sicherheitsrisiken

Der Lieferant muss Sicherheitsrisiken in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit identifizieren und bewerten und auf der Grundlage dieser Bewertung geeignete technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten.

Der Lieferant bewertet periodisch die Risiken im Zusammenhang mit Informationssystemen und der Verarbeitung, Speicherung und Übertragung von Informationen.

2. Sicherheitsrisikomanagement für personenbezogene Daten

Der Lieferant muss Sicherheitsrisiken in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit ermitteln und bewerten und auf der Grundlage dieser Bewertung geeignete technische und organisatorische Maßnahmen ergreifen, um ein Sicherheitsniveau zu gewährleisten, das dem Risiko der spezifischen Arten und Zwecke personenbezogener Daten, die vom Lieferanten verarbeitet werden, angemessen ist:

- die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten;
- die Fähigkeit, die laufende Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten zu gewährleisten;
- die Fähigkeit, die Verfügbarkeit und den Zugang zu den Daten des Käufers im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen;
- ein Verfahren zur regelmäßigen Prüfung, Beurteilung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung .

Der Lieferant bewertet regelmäßig die Risiken im Zusammenhang mit Informationssystemen und der Verarbeitung, Speicherung und Übertragung persönlicher Daten.

Organisation der Informationssicherheit

Der Lieferant muss über definierte und dokumentierte Sicherheitsrollen und -verantwortlichkeiten innerhalb seiner Organisation verfügen.

Der Lieferant muss mindestens eine Person benennen, die über angemessene Sicherheitskompetenz verfügt und die die Gesamtverantwortung für die Umsetzung der Sicherheitsmaßnahmen im Rahmen der Richtlinie zur Datensicherheit trägt und die die Kontaktperson für das Sicherheitspersonal des Käufers sein wird.

Gewährleistung der Datensicherheit durch das Personal

Der Lieferant stellt sicher, dass sein Personal Informationen gemäß dem in der Vereinbarung geforderten Vertraulichkeitsgrad behandelt.

Der Lieferant stellt sicher, dass sein zuständiges Personal über die genehmigte Nutzung (gegebenenfalls einschließlich Nutzungsbeschränkungen) von Informationen, Einrichtungen und Systemen im Rahmen der Vereinbarung informiert ist. Der Käufer hat das Recht, von jedem einzelnen Personal des Lieferanten eine unterzeichnete Quittung zu verlangen, die bestätigt, dass es die

Sicherheitsrichtlinien und die genehmigte Nutzung von Informationen, Systemen und Einrichtungen verstanden hat und einhalten wird.

Der Lieferant stellt sicher, dass sein Personal, das Aufträge im Rahmen der Vereinbarung ausführt, vertrauenswürdig ist, festgelegte Sicherheitskriterien erfüllt und einer angemessenen Überprüfung und Hintergrundüberprüfung unterzogen wurde und während der Dauer des Auftrags weiterhin unterzogen wird.

Der Lieferant darf ohne vorherige Information und schriftliche Genehmigung des Käufers kein Personal des Lieferanten für den Auftrag des Käufers abstellen, das

- einen Interessenkonflikt in Bezug auf den Käufer oder den betreffenden Auftrag hat; oder
- in den drei (3) Jahren vor dem Einsatz oder der Entsendung zu einer Gefängnisstrafe wegen einer Straftat verurteilt worden ist

Der Käufer muss Informationen darüber bereitstellen, welche Aufgaben zum Zeitpunkt des Vertragsabschlusses oder spätestens zwei Wochen vor Beginn des Personaleinsatzes oder -einsatzes des Lieferanten als sensibel eingestuft werden.

Der Lieferant muss sicherstellen, dass sein Personal mit Sicherheitsaufgaben angemessen geschult ist, um sicherheitsbezogene Aufgaben auszuführen.

Der Lieferant muss für sein zuständiges Personal regelmäßig Schulungen zum Sicherheitsbewusstsein durchführen oder sicherstellen. Eine solche Schulung des Lieferanten muss unter anderem Folgendes umfassen:

- Wie man mit der Sicherheit von Kundeninformationen umgeht (d.h. Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen);
- Warum Informationssicherheit notwendig ist, um die Informationen und Systeme der Kunden zu schützen;
- Die häufigsten Arten von Sicherheitsbedrohungen (wie Identitätsdiebstahl, Malware, Hacking, Informationslecks und Insider-Bedrohungen);
- Die Bedeutung der Einhaltung von Informationssicherheitsrichtlinien und der Anwendung der damit verbundenen Standards/Verfahren;
- Persönliche Verantwortung für die Informationssicherheit (z.B. Schutz der privatsphärenbezogenen Informationen des Kunden und Meldung tatsächlicher und vermuteter Sicherheitsvorfälle).

Vermögensverwaltung

Der Lieferant muss über ein definiertes und dokumentiertes Asset-Management-System verfügen und aktuelle Aufzeichnungen über alle relevanten Vermögenswerte und deren Eigentümer führen. Zu den Informationsgütern gehören unter anderem IT-Systeme, Sicherungs- und/oder Wechselmedien mit sensiblen Informationen, Zugriffsrechte, Software und Konfiguration.

Der Lieferant kennzeichnet, behandelt und schützt Informationen gemäß einem vordefinierten Informationsklassifikationssystem in Übereinstimmung mit den zu diesem Zeitpunkt gültigen Sicherheitsstandards (einschließlich Speicherung auf Wechselmedien, Entsorgung und physische Übertragung).

Der Lieferant muss Maßnahmen ergreifen, um den Schutz vor zufälligem, unbefugtem oder unrechtmäßigem Verlust, Zerstörung, Änderung oder Beschädigung der übertragenen, gespeicherten oder anderweitig verarbeiteten Daten des Käufers zu gewährleisten.

Der Lieferant muss eine aktualisierte Liste der verarbeiteten Daten des Käufers führen. Die Liste muss die folgenden Informationen enthalten:

- die verarbeiteten Daten;

- Speicherdetails, wie z.B. Name des Assets, Standort usw.
-

Zugangskontrolle

Der Lieferant muss über eine definierte Zugangskontrollpolitik für Einrichtungen, Standorte, Netzwerk, System, Anwendung und Informations-/Datenzugang (einschließlich physischer, logischer und Fernzugangskontrollen), ein Autorisierungsverfahren für Benutzerzugang und -privilegien, Verfahren zum Widerruf von Zugangsrechten und eine akzeptable Nutzung von Zugangsprivilegien für das Personal des Lieferanten verfügen.

Der Lieferant muss einen formellen Benutzeran- und -abmeldeprozess implementieren lassen, um die Zuweisung von Zugriffsrechten zu ermöglichen.

Der Anbieter vergibt alle Zugriffsprivilegien auf der Grundlage des Prinzips "need-to-know" und des Prinzips "least privilege".

Der Anbieter verwendet eine starke Authentifizierung (Multi-Faktor-Authentifizierung) für Fernzugriffsbenutzer und Benutzer, die sich über ein nicht vertrauenswürdiges Netzwerk verbinden.

Der Lieferant muss sicherstellen, dass sein Personal über eine persönliche und eindeutige Kennung (Benutzer-ID) verfügt und eine geeignete Authentifizierungstechnik verwendet, die die Identität der Benutzer bestätigt und sicherstellt.

Physische und ökologische Sicherheit

Der Lieferant schützt die Informationsverarbeitungseinrichtungen vor externen und umweltbedingten Bedrohungen und Gefahren, einschließlich Strom-/Verkabelungsausfällen und anderen Unterbrechungen, die durch Ausfälle der unterstützenden Versorgungseinrichtungen verursacht werden. Dazu gehören der physische Perimeter und der Zugangsschutz.

Der Lieferant schützt Waren, die er im Namen des Käufers erhält oder versendet, vor Diebstahl, Manipulation und Zerstörung.

Sicherheit im Betrieb

Der Lieferant muss über ein etabliertes Änderungsmanagementsystem verfügen, um Änderungen an Geschäftsprozessen, Informationsverarbeitungseinrichtungen und -systemen vornehmen zu können. Das Änderungsmanagementsystem muss Tests und Überprüfungen umfassen, bevor Änderungen implementiert werden, wie z.B. Verfahren zur Behandlung dringender Änderungen, Rollback-Verfahren zur Wiederherstellung nach fehlgeschlagenen Änderungen, Protokolle, aus denen hervorgeht, was, wann und von wem geändert wurde.

Der Lieferant muss einen Malware-Schutz implementieren, um sicherzustellen, dass jede Software, die für die Bereitstellung der Liefergegenstände durch den Lieferanten an den Käufer verwendet wird, vor Malware geschützt ist.

Der Lieferant erstellt Sicherungskopien von kritischen Informationen und testet Sicherungskopien, um sicherzustellen, dass die Informationen wie mit dem Käufer vereinbart wiederhergestellt werden können.

Der Lieferant protokolliert und überwacht Aktivitäten, wie das Erstellen, Lesen, Kopieren, Ändern und Löschen von verarbeiteten Daten sowie Ausnahmen, Fehler und Informationssicherheitsereignisse und überprüft diese regelmäßig. Darüber hinaus schützt und speichert der Lieferant (für mindestens 6 Monate oder in Übereinstimmung mit den örtlichen Gesetzen) Protokollinformationen und liefert auf

Anfrage Überwachungsdaten an den Käufer. Anomalien / Vorfälle / Indikatoren für Kompromisse müssen gemäß den Anforderungen des Vorfallmanagements gemeldet werden.

Der Lieferant muss die Schwachstellen aller relevanten Technologien wie Betriebssysteme, Datenbanken und Anwendungen proaktiv und rechtzeitig angehen.

Der Anbieter muss Sicherheitsbasislinien (Härtung) für alle relevanten Technologien wie Betriebssysteme, Datenbanken und Anwendungen festlegen.

Der Lieferant muss sicherstellen, dass die Entwicklung von der Test- und Produktionsumgebung getrennt ist.

Sicherheit der Kommunikation

Der Lieferant muss Netzwerksicherheitskontrollen wie Service-Level, Firewalling und Segregation implementieren, um Informationssysteme zu schützen.

Systemerwerb, -entwicklung und -wartung (wenn die Software- oder Systementwicklung dem Käufer von telXira zur Verfügung gestellt wird)

Der Lieferant muss Regeln für den Entwicklungslebenszyklus von Software und Systemen einschließlich Änderungs- und Überprüfungsverfahren einführen.

Der Lieferant muss die Sicherheitsfunktionalität während der Entwicklung in einer kontrollierten Umgebung testen.

Die Lieferantenbeziehung mit Unterlieferanten

Der Lieferant muss den Inhalt dieser Richtlinie zur Datensicherheit in seinen Vereinbarungen mit Unterlieferanten, die im Rahmen der Vereinbarung zugewiesene Aufgaben ausführen, widerspiegeln.

Der Lieferant muss die Einhaltung der Richtlinie zur Datensicherheit durch den Unterlieferanten regelmäßig überwachen, überprüfen und auditieren.

Management von Sicherheitsvorfällen

Der Lieferant muss über festgelegte Verfahren für das Management von Sicherheitszwischenfällen verfügen.

Der Lieferant informiert den Käufer so bald wie möglich, spätestens jedoch innerhalb von 24 Stunden nach Feststellung des Sicherheitsvorkommnisses (einschließlich, aber nicht beschränkt auf Vorfälle im Zusammenhang mit der Verarbeitung personenbezogener Daten) über jedes Sicherheitsvorkommnis.

Alle Berichte über sicherheitsrelevante Vorfälle sind als vertrauliche Informationen zu behandeln und mit branchenüblichen Verschlüsselungsmethoden wie PGP (Pretty Good Privacy Encryption) zu verschlüsseln.

Der Bericht über den Sicherheitsvorfall muss mindestens die folgenden Informationen enthalten:

- Ungeachtet des Erfordernisses einer sofortigen Benachrichtigung muss der Lieferant dem Käufer einen schriftlichen Vorbericht über jedes Sicherheitsvorkommnis vorlegen, das den Käufer oder die Vermögenswerte des Käufers in irgendeiner vorstellbaren Weise beeinträchtigen könnte;

- Abfolge der Ereignisse, einschließlich der während der Behandlung des Vorfalls ergriffenen Maßnahmen;
- betroffene Teile der Infrastruktur, Systeme und Informationen;
- geschätzte (oder, bei einem hohen Maß an Unsicherheit, schlimmstmögliche) Folgen/Auswirkungen;
- bereits eingeführte Maßnahmen zur Verringerung der Folgen;
- risikoreduzierende Maßnahmen bereits umgesetzt;
- Maßnahmen zur Reduzierung der Folgen, die umgesetzt werden müssen, einschließlich des Umsetzungsplans (Datum; verantwortlich; Abhängigkeiten);
- umzusetzende risikomindernde Maßnahmen, einschließlich eines Umsetzungsplans (Datum; verantwortlich; Abhängigkeiten);
- Zusammenfassung der Erfahrungen

Einhaltung der Vorschriften

Der Lieferant muss alle relevanten Gesetze und vertraglichen Anforderungen einhalten, einschließlich, aber nicht beschränkt auf den Schutz personenbezogener Daten.

Der Lieferant stellt dem Käufer auf Anfrage ohne ungerechtfertigte Verzögerung einen Bericht über den Stand der Einhaltung dieser Richtlinie zur Datensicherheit zur Verfügung.