Technisch-Organisatorische Maßnahmen
enSecure Site/Net/Cloud

Die hier beschriebenen technischen und organisatorischen Maßnahmen werden festgelegt zwischen dem Auftraggeber und envia TEL GmbH (Auftragnehmer, im Folgenden „envia TEL“ genannt).

1 Allgemeine Anforderungen der Informationssicherheit

1.1 Seriöse Quellen

envia TEL stellt sicher, dass Hard- und Softwareprodukte aus bekannten und seriösen Quellen bezogen werden und dass es einen zuverlässigen technischen Support und eine nachvollziehbare Lieferkette gibt.

1.2 Sicherheits-Governance

envia TEL erstellt, pflegt und überwacht ein Governance-Rahmenwerk für die Informationssicherheit.

1.3 Management von Informationssicherheitsrisiken

envia TEL stellt sicher, dass vor (i) der Einführung neuer IT-Umgebungen, in denen Informationen des Auftraggebers einschließlich personenbezogener Daten (im Folgenden „Auftraggeber Informationen“) gespeichert sind, (ii) der Implementierung wesentlicher Änderungen an bestehenden IT-Umgebungen, und (iii) der Einführung neuer Technologien die hiermit einhergehenden Informationssicherheitsrisiken identifiziert, bewertet, behandelt, überwacht und in akzeptablen Grenzen gehalten werden.

1.4 Sicherheitsmanagement

envia TEL hat (i) eine spezialisierte Informationssicherheitsfunktion eingerichtet, um sicherzustellen, dass bewährte Praktiken zur Informationssicherheit im gesamten Unternehmen wirksam und konsequent angewandt werden und dass die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen, die die Informationssicherheit betreffen, gewährleistet ist. envia TEL betreibt (ii) ein umfassendes, kontinuierliches Security Awareness Programm, um für das erwartete Sicherheitsverhalten bei allen Personen, die Zugang zu Auftraggeber Informationen haben, zu werben.

1.5 Dokumentierte Betriebsprozesse

envia TEL hat Zuständigkeiten und Verfahren für die Verwaltung und den Betrieb seiner Dienstleistungen festgelegt, um sicherzustellen, dass diese Dokumentation (i) den anerkannten Branchenstandards und Best Practices entspricht, (ii) sachgemäß schriftlich dokumentiert ist und (iii) während der Laufzeit dieser Vereinbarung stets auf einem aktuellen Stand ist.

1.6 Verwaltung von Betriebsmitteln

envia TEL stellt sicher, dass (i) Betriebsmittel (Hardware und Software, im Folgenden „Betriebsmittel“ genannt), die zur Erstellung, Verarbeitung, Speicherung oder Übertragung von Auftraggeber Informationen verwendet werden, während ihres gesamten Lebenszyklus vor Korruption, Verlust, Diebstahl und unbefugter Offenlegung geschützt sind. envia TEL stellt sicher, dass diese Betriebsmittel in Inventarlisten erfasst sind, die (ii) gegen unbefugte Änderungen geschützt sind, (iii) aktuell gehalten werden, (iv) regelmäßig gesichert werden und (v) die erforderlichen Angaben über die Betriebsmittel enthalten. envia TEL stellt sicher, dass (vi) alle Betriebsmittel einem Verantwortlichen zugeordnet werden, der für den Betrieb der Betriebsmittel verantwortlich ist.

1.7 Physische Sicherheit

envia TEL trifft angemessene Vorkehrungen zur physischen Sicherheit und zum Zutrittsschutz der bei envia TEL gehosteten Betriebsmittel. Insbesondere sind Maßnahmen zum Schutz gegen Feuer und Wasser, zum Schutz vor bzw. Vermeidung von extremen Temperaturen und zur Notstromversorgung implementiert. Zutritt zu Bereichen mit Auftraggeber Informationen oder Betriebsmitteln, die Auftraggeber Informationen verarbeiten oder Prozesse unterstützen, die Auswirkungen auf die Sicherheit von Auftraggeber Informationen haben, sind auf einen autorisierten Personenkreis beschränkt (Least Privilege). Dazu gehören auch die Zutrittsschutzmaßnahmen für Rechenzentren inklusive Überwachung der kritischen Bereiche, Zutrittsprotokolle, Zutritt von Fremdfirmenmitarbeitern in Begleitung und Sicherung gegen Einbruch.

Betriebsmittel, welche vor Ort beim Kunden eingesetzt werden, müssen analog der soeben beschriebenen Maßnahmen geschützt werden. Insbesondere muss der Kunde den sicheren Betrieb der Betriebsmittel durch einen geeigneten, abgeschlossenen Ort gewährleisten. envia TEL hat Maßnahmen ergriffen, um auch für beim Kunden eingesetzte Betriebsmittel einen unbefugten administrativen Zugriff zu verhindern (kein lokaler Zugriff auf die Administrationsoberfläche der Betriebsmittel). Zum Schutz des Kundennetzwerkes müssen diese Betriebsmittel zudem zur erstmaligen Nutzung durch den Kunden manuell im zentralen Managementsystem der envia TEL (FortiManager) aktiviert werden und sind ebenso vor der Rückgabe an envia TEL zu deaktivieren.

1.8 Systemzugang/-zugriff

envia TEL beschränkt den Zugang zu bzw. Zugriff auf Betriebsmittel, mit denen Auftraggeber Informationen erstellt, verarbeitet, gespeichert oder übertragen werden, auf autorisiertes Personal für zweckgebundene betriebliche Zwecke. Dazu gehört, dass (i) nur autorisiertes Personal Zugang zu bzw. Zugriff auf Auftraggeber Informationen erhalten, (ii) die Zugriffsrechte auf die genehmigte Systemfunktionalität beschränkt sind, (iii) eine angemessene Funktionstrennung besteht, und (iv) die Zugriffsrechte nicht geteilt werden (Benutzer-IDs und Passwörter dürfen nicht geteilt werden). envia TEL stellt sicher, dass der administrative Zugriff auf Systeme, die Auftraggeber Informationen speichern oder verarbeiten, (v) auf eine minimale Anzahl

von Administratoren beschränkt ist. envia TEL stellt weiterhin sicher, dass der administrative Zugriff (vi) immer protokolliert wird, um unberechtigten Zugriff auf und/oder unberechtigte Manipulation von Auftraggeber Informationen erkennen und untersuchen zu können. (vii) Zudem stellt envia TEL sicher, dass ein formales Verfahren eingerichtet und aufrechterhalten wird, das beschreibt, wie Rollen, Konten, Zugriffsrechte und Berechtigungen für den administrativen Zugriff erstellt, regelmäßig überprüft, geändert, gesperrt und/oder gelöscht werden.

1.9 Systemverwaltung

envia TEL betreibt Systeme, die Auftraggeber Informationen erstellen, speichern, verarbeiten oder übertragen, um (i) die aktuelle und prognostizierte Auslastung zu bewältigen und (ii) sie konsistent und fehlerfrei zu konfigurieren, um sie und die Auftraggeber Informationen, die sie verarbeiten, speichern oder übertragen, vor Fehlfunktionen, Cyberangriffen, unbefugter Offenlegung, Korruption, Diebstahl und Verlust zu schützen. envia TEL verwaltet die Sicherheit der Systeme, indem (iii) Backups von Informationen und Software durchgeführt werden, (iv) ein Änderungsmanagement-Prozess angewendet wird, und (v) die Einhaltung vereinbarter Service Level Agreements überwacht werden.

1.10 Netzwerk und Kommunikation

envia TEL stellt sicher, dass physische, drahtlose und – falls zutreffend – Sprachnetze so ausgelegt sind, dass sie (i) zuverlässig und belastbar sind, (ii) unberechtigten Zugriff verhindern, (iii) verschlüsselte Verbindungen verwenden, und (iv) verdächtigen Datenverkehr erkennen. (v) envia TEL stellt sicher, dass Netzwerkgeräte so konfiguriert sind, dass sie nach Bedarf funktionieren und nicht autorisierte und fehlerhafte Updates verhindern. envia TEL gewährleistet den Schutz elektronischer Kommunikationssysteme, indem (vi) Richtlinien für deren Verwendung festgelegt sind, (vii) Sicherheitseinstellungen konfiguriert sind und (viii) die unterstützende technische Infrastruktur abgesichert ist. (ix) envia TEL stellt sicher, dass Computer- und Netzwerknamen und -topologien vor Dritten verborgen bleiben. envia TEL sichert zu, den externen Zugriff auf Informationssysteme und Netzwerke einzuschränken, indem (x) Demilitarisierte Zonen (DMZs) zwischen nichtvertrauenswürdigen Netzwerken und internen Netzwerken eingerichtet sind, (xi) der Netzwerkverkehr durch Firewalls oder Proxy-Firewalls geleitet wird, (xii) die Verbindungarten auf ein erforderliches Minimum beschränkt sind, und (xiii) der Zugriff nur auf autorisierte Geschäftsanwendungen, Informationssysteme oder bestimmte Teile des Netzwerks gewährt ist.

1.11 Technisches Sicherheitsmanagement

envia TEL installiert Malware-Schutzlösungen auf Systemen, auf denen Auftraggeber Informationen Malware ausgesetzt sein können, einschließlich (i) Servern (z. B. Applikationsserver, Databankserver, Fileserver, Printserver, Webserver) und (ii) Computergeräten (z. B. Desktop-Computern, Laptops und anderen mobilen Geräten). (iii) Die Malware-Schutzsoftware schützt vor allen Formen von Malware (z. B. Viren, Würmern, Trojanischen Pferde, Spyware, Rootkits, Botnet-Software, Keylogger, Ransomware). envia TEL stellt sicher und überprüft, dass (iv) die Malware-Schutzsoftware nicht deaktiviert oder in der Funktion eingeschränkt wurde, (v) die Konfiguration der Malware-Schutzsoftware korrekt ist, (vi) Updates innerhalb definierter Zeiträume korrekt angewendet werden, (vii) Scans zu festgelegten Zeiten durchgeführt werden, und (viii) eine Benachrichtigung über identifizierte Malware-Ereignisse erfolgt.

1.12 Trennung von Test- und Produktivsystemen

envia TEL stellt sicher, dass (i) Test- und Produktivsysteme zumindest logisch getrennt sind, um das Risiko eines unbefugten Zugriffs oder einer unbefugten Veränderung der Produktivsysteme zu reduzieren. (ii) Sollte eine Trennung nicht möglich sein, stellt envia TEL sicher, dass speziell angepasste Verfahren für den Prozess zum Änderungsmanagement und zum Management von Informationssicherheitsvorfällen festgelegt werden, um schnell und angemessen auf Störungen und Probleme in den Produktivsystemen reagieren zu können. (iii) Produktivdaten sind in Test- und Entwicklungsumgebungen nicht erlaubt und müssen anonymisiert werden, wenn sie personenbezogene Daten oder die Möglichkeit der Korrelation personenbeziehbarer Daten enthalten.

1.13 Scanning auf Schwachstellen

envia TEL leistet Hilfe für und unterstützt Sicherheits- und Schwachstellen-Scans, die vom Auftraggeber durchgeführt werden.

1.14 Aktuelle Patch Level

envia TEL stellt sicher, dass technische Schwachstellen behoben werden, indem ein Patch-Management-Prozess betrieben wird, der sicherstellt, dass (i) Patches identifiziert und von autorisierten Quellen bezogen werden, sobald sie verfügbar sind, (ii) entschieden wird, wann Patches bereitgestellt werden, (iii) Patches anhand bekannter Kriterien getestet werden und (iv) Patches rechtzeitig bereitgestellt werden. (v) envia TEL ist befugt, Patches in der IT-Umgebung anzuwenden, einschließlich Virtualisierungshypervisoren, virtuellen Maschinen, Betriebssystemen und Anwendungen, solange dies keine negativen Auswirkungen auf die Vertraulichkeit, Integrität oder Verfügbarkeit von Auftraggeber Informationen hat.

1.15 Mindestanforderungen für Anmeldeinformationen

envia TEL stellt sicher, dass die Mindestanforderungen für Anmeldeinformationen (Zwei-Faktor Authentifizierung) für die IT-Umgebung, in der Auftraggeber Informationen gespeichert oder verarbeitet werden, gewährleistet sind. Rollenbasierte Berechtigungskonzepte halten die Grundsätze „Least Privilege“, „Need-to-know“ und „Segregation of Duties“ ein.

1.16 Netzwerkdesign

envia TEL verwendet eine mehrschichtige Netzwerkarchitektur sowie Demilitarisierte Zonen (DMZ) für Anwendungen, die über das Internet erreichbar sind. Netzwerksegmente sind mit geeigneten Sicherheitsmaßnahmen voneinander getrennt, um den Datenverkehr zwischen den Segmenten zu verhindern.

1.17 Fernzugriffe und mobiles Arbeiten

envia TEL stellt sicher, dass Fernzugriffsmöglichkeiten nach aktuellem Stand der Technik geschützt sind. Mobiles Arbeiten von envia TEL Mitarbeitern erfolgt nur unter der Maßgabe, dass die Mitarbeiter geschult und schriftlich zur Einhaltung datenschutzrechtlicher und betrieblicher Bestimmungen verpflichtet wurden. envia TEL stellt seinen Mitarbeitern hierfür Soft- und Hardware zur Verfügung, die nur für dienstliche Zwecke genutzt werden darf. Vertrauliche Unterlagen sind vor Dritten zugriffsgeschützt verwahrt, eine Entsorgung von Unterlagen erfolgt nur in den Räumen der envia TEL im Rahmen einer datenschutzkonformen Entsorgung/Vernichtung. Die vereinbarten Sicherheitsmaßnahmen werden auch bei Erbringung der Leistung in mobiler Arbeit eingehalten. Ein Mithören und Mitlesen durch Unbefugte muss hierbei ausgeschlossen sein.

1.18 Verschlüsselung

Data-at-Rest und Data-in-Motion (in-Transit) werden nur über sichere Protokolle und mittels einer state-of-the-art Verschlüsselung gespeichert und übertragen. Authentisierungsmerkmale (Passwörter, PINs) werden nur verschlüsselt über das Netzwerk übermittelt.

1.19 Härtung

Alle Informations- und Netzwerksysteme werden gehärtet. Dies beinhaltet (i) das Deaktivieren unnötiger Anwendungen, Dienste, Tools, Protokolle und Schnittstellen, (ii) das Löschen oder zumindest Ändern der vom Hersteller bereitgestellten Standardbenutzernamen und Passwörter, (iii) das Aktivieren von sicherheitserhöhenden Optionen und (iv) das Verhindern der Übertragung von technischen Informationen an externe Stellen.

1.20 Protokollierung von Sicherheitsereignissen

Um die Erkennung und Untersuchung von unbefugtem Zugriff auf und unbefugten Manipulation von Auftraggeber Informationen zu ermöglichen, stellt envia TEL sicher, dass (i) die Ereignisprotokollierung jederzeit für alle von envia TEL betriebenen Systeme zum Erstellen, Speichern, Verarbeiten oder Übertragen von Auftraggeber Informationen aktiviert ist, (ii) Systeme so konfiguriert sind, dass sie sicherheitsrelevante Ereignisse und Ereignisse mit Relevanz für die Datenintegrität (einschließlich Ereignistypen wie Änderungen an Auftraggeber Informationen, erfolgreiche und fehlgeschlagene Benutzeranmeldeversuche, Erstellung/Änderung/Löschen von Diensten, Erstellung/Änderung/Löschen von Objekten, Systemabstürze, Löschen von Benutzerkonten) und mit jedem Ereignis verbundene Ereignisattribute (z. B. Datum, Uhrzeit, Benutzer-ID, Dateiname und IP-Adresse) erzeugen, (iii) konsistente, vertrauenswürdige Datums- und Zeitquellen sicherstellen, dass Ereignisprotokolle korrekte Zeitstempel verwenden, (iv) sicherheits- und integritätsrelevante Ereignisprotokolle vor unbefugten Zugriff und versehentlicher oder absichtlicher Änderung bzw. Überschreibung geschützt sind.

1.21 Compliance-Management

envia TEL stellt sicher, dass (i) alle Systeme, die Auftraggeber Informationen erstellen, speichern, verarbeiten oder übertragen, regelmäßig auf Einhaltung der eigenen Sicherheitsrichtlinien überprüft werden. (ii) Die Sicherheitsrichtlinien von envia TEL sind im Einklang mit den in den Abschnitten 2 und 3 dieser Anlage genannten Standards.

1.22 Sichere Entsorgung und Wiederverwendung

envia TEL stellt sicher, dass ausrangierte Hardware (i) entweder vor der Wiederverwendung, dem Verkauf oder der Rückgabe so gesäubert wird, dass alle Auftraggeber Informationen sicher gelöscht werden (ii) oder sicher vernichtet werden. (iii) Die Säuberung oder Vernichtung wird auf sichere Weise dem Stand der Technik entsprechender Technologien, Verfahren und Werkzeugen durchgeführt.

1.23 Personalsicherheit

envia TEL gewährleistet einen Identitätsnachweis für natürliche Personen, die im Auftrag von envia TEL handeln, und dass niemand den Zugang/Zugriff oder die von envia TEL gewährten Berechtigungen missbraucht. envia TEL stellt sicher, dass die gewährten Berechtigungen nach Kündigung oder Wechsel von Personen und/oder Verantwortlichkeiten unverzüglich entzogen werden. envia TEL beauftragt nur Personal, das für die durchzuführenden Aufgaben qualifiziert ist.

1.24 Sicherheit in der Lieferkette

envia TEL stellt sicher, dass Informationssicherheitsrisiken in jeder Phase der Beziehungen zu externen Lieferanten von Hard- und Software über die gesamte Lieferkette identifiziert und gemanagt werden, indem (i) die Anforderungen bezüglich Informationssicherheit in formale Verträge eingebunden sind und (ii) sichergestellt wird, dass diese erfüllt sind. (iii) envia TEL stellt sicher, dass Subunternehmer, die an der Verarbeitung, Speicherung, Übermittlung oder Entsorgung von Auftraggeber Informationen beteiligt sind, mindestens die in dieser Anlage vereinbarten Anforderungen erfüllen. (iv) envia TEL ist für eine angemessene Steuerung des/der Subunternehmer(s) sowie für die Einhaltung der ausgelagerten Kontrollen verantwortlich.

envia TEL GmbH
Geschäftsanschrift Friedrich-Ebert-Straße 26 · 04416 Markkleeberg · T 0800 0101600 · F 0800 3684283
www.enviaTEL.de · info@enviaTEL.de · **Geschäftsführung** Stephan Drescher · **Sitz der Gesellschaft** Markkleeberg
Registergericht Amtsgericht Leipzig · HRB 24812 · **USt-ID-Nr.** DE183563546

2 Datenschutz

2.1 Verpflichtung zur Vertraulichkeit

envia TEL verpflichtet alle Mitarbeiter, die personenbezogene Daten des Auftraggeberes verarbeiten oder Zugriff hierauf haben, schriftlich zur Vertraulichkeit beim Umgang mit personenbezogenen Daten. Sofern auftragsbezogen oder gesetzlich erforderlich, verpflichtet envia TEL die Mitarbeiter darüber hinaus schriftlich auf das Fernmeldegeheimnis (Gem. ePrivacy-Richtlinie oder -Verordnungen in ihrer jeweils gültigen Fassung i. V. m. nationalen Regelungen zum Fernmeldegeheimnis, z.B. § 88 TKG für Deutschland).
envia TEL schult alle Mitarbeiter, die personenbezogene Daten des Auftraggebers verarbeiten oder Zugriff hierauf haben, zur Datensicherheit und zum Datenschutz. Die Teilnahme wird namensscharf dokumentiert.

2.2 Datenschutz durch Technikgestaltung

envia TEL trifft Regelungen zum „Datenschutz durch Technikgestaltung“, um das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen (bspw. durch Maßnahmen wie Datenminimierung, Pseudonymisierung, datenschutzfreundliche Voreinstellungen) zu berücksichtigen.

3 Standards

Für envia TEL bestehen zurzeit folgende Zertifikate/Datenschutzkonzepte:

- ISO 27001
- ISO 9001

envia TEL stellt alle Zertifikate/Datenschutzkonzepte in der aktuell gültigen Form auf der Webseite www.enviatel.de zur Verfügung.

4 Prozessschnittstellen der Informationssicherheit

Beide Parteien verpflichten sich, Ansprechpartner für Informationssicherheitsprozesse zu benennen und zur Verfügung zu stellen und vereinbaren eine gemeinsame Zusammenarbeit und einen Informationsaustausch innerhalb dieser Sicherheitsprozesse.