Technische und organisatorische Maßnahmen zum Datenschutz

DEMANDA Inkassomanagement und –service GmbH

(im Folgenden kurz „DEMANDA“)

1. EINLEITUNG

1.1. Mit diesem Dokument werden die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten im Rahmen der Tätigkeiten der DEMANDA beschrieben.

1.2. Die technischen und organisatorischen Maßnahmen werden fortwährend sowohl an die aktuelle Rechtslage des Datenschutzes als auch entsprechend dem aktuellen „Stand der Technik“ angepasst.

1.3. Personenbezogene Daten werden bei DEMANDA in einer Art und Weise verarbeitet, die

a) die **Vertraulichkeit** wahrt (nur Berechtigte erhalten Zugriff)

b) die **Integrität** erhält (nur Berechtigte können Änderungen durchführen)

c) die **Verfügbarkeit** gewährt (wenn personenbezogene Daten aufgrund vertraglicher Grundlagen innerhalb von DEMANDA gespeichert werden, bleiben diese Daten wie vertraglich geregelt verfügbar)

1.4. Alle Mitarbeiter von DEMANDA sind verpflichtet, sich an die Vorgaben des vorliegenden Dokuments über „Technisch-Organisatorische Maßnahmen zum Datenschutz“ und der dazugehörigen Sicherheitsstandards zu halten. Zudem sind bildet die Datenschutzrichtlinie der DEMANDA die Grundlage für einen vertrauensvollen Umgang mit personenbezogenen Daten.

2. TECHNISCH-ORGANISATORISCHE MAßNAHMEN

In den nachfolgenden Abschnitten werden die aktuellen Sicherheitsmaßnahmen definiert. Für DEMANDA ist es ein Anliegen, diese jederzeit zu verbessern oder zu erhöhen, und behält sich das Recht vor, dies jederzeit zu tun. Dies kann dazu führen, dass einzelne Maßnahmen durch andere ersetzt werden, die jedoch dem gleichen Sicherheitsziel dienen.

2.1. VERTRAULICHKEIT, PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG

2.1.1. Zugangskontrolle:

DEMANDA setzt nachstehende Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

Es werden mehrere Ebenen der Autorisierung genutzt, um Zugang zu sensitiven Systemen zu gewähren. Es existieren Prozesse, die erfordern, dass Mitarbeiter nur aufgrund entsprechender Genehmigung hinzugefügt, gelöscht oder angepasst werden. Die Berechtigung wird direkt von der Geschäftsführung eingeräumt bzw. von der Geschäftsführung entzogen.

Alle Mitarbeiter greifen auf die Systeme der DEMANDA Inkassamanagement und-service GmbH mit individuellen User-IDs zu.

DEMANDA hat Prozesse, die sicherstellen, dass beantragte Änderungen an Berechtigungen gemäß den Richtlinien geführt werden (zB werden keine Rechte ohne Genehmigung vergeben).

Verlässt ein Mitarbeiter das Unternehmen, werden sämtliche Zugriffsrechte entzogen.

DEMANDA erteilt seinen Mitarbeitern Weisungen über das regelmäßige Ändern von Passwörtern.

Es werden personalisierte User-IDs zur Authentifizierung vergeben. Passwörter werden verschlüsselt gespeichert. Es entspricht den Anforderungen an komplexe Passwörter. DEMANDA stellt sicher, dass Default-Passwörter vor Inbetriebnahme geändert werden.

Mitarbeiter von DEMANDA wurden entsprechend sensibilisiert, technische Geräte, wie Firmenlaptops nicht unbeaufsichtigt bzw. ungeschützt im Betrieb zu lassen. Darüber erfolgt ein zeitlich festgelegter automatischer Logout aus dem DEMANDA System.

Das Firmennetzwerk ist ein virtuelles Private-Cloud Netzwkerk und gegen das öffentliche Netzwerk durch eine Firewall geschützt.

DEMANDA verwendet Virenscanner an den Übergängen zum Firmennetz (Email-Account), sowie auf allen Fileservern und auf allen Einzelplatzcomputern.

Sicherheitsrelevante Softwareupdates werden regelmäßig und automatisiert in die vorhandene Software eingespielt.

Es ist Mitarbeitern nicht gestattet, Daten von DEMANDA auf externen Datenträgern (USB-Sticks, Festplatten) zu speichern.

Die Geschäftsführung verwendet ein gemeinsames Microsoft oneDrive-Verzeichnis, auf dem interne Dokumentationen und Verträge abgelegt werden. Weder Assistenz noch sonstige Mitarbeiter haben hierauf Zugriff.

Mitarbeiter von DEMANDA verwenden primär Firmenlaptops, die mit den in diesem Dokument ersichtlichen, strengen Sicherheitsmaßnahmen ausgestattet sind.

Wenn Mitarbeiter andere Geräte für den Zugriff verwenden darf lediglich das DEMANDA Portal über einen autorisierten Browser (Google Chrome in der aktuellsten Version) verwendet werden. Die Dokument und Daten aus dem DEMANDA-Portal dürfen nie auf lokale Datenträger abgespeichert werden. Die Geschäftsprozesse von DEMANDA sind so gestaltet, dass dies auch in aller Regel nicht nötig ist.

2.1.2. Zugriffskontrolle:

DEMANDA gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen und Mitarbeiter ausschließlich auf die – ihrer Zugriffsberechtigung unterliegenden – Daten zugreifen können und dass die personenbezogenen Daten im Zuge der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Folgende Maßnahmen werden gesetzt:

Der Zugriff auf personenbezogene, vertrauliche oder anderweitig sensitive Information ist beschränkt auf Personen, die zu diesem Zugriff aufgrund ihrer Leistungserbringung befugt werden. Mitarbeiter erhalten dabei lediglich Zugriff auf die Informationen, die sie zur Erledigung der Arbeitsaufgabe benötigen. Hierzu verwendet DEMANDA Berechtigungskonzepte. Die Mitarbeiter werden in die Nutzergruppen Mitarbeiter und Administrator eingeteilt. Mitarbeiter können lediglich auf die personenbezogenen Daten von ihnen zugeordneten Fällen zugreifen. Die Nutzergruppe Administrator ist der Geschäftsführung vorbehalten und gewährt Zugriff auf alle Fälle samt zugehöriger personenbezogener Daten.

Alle personenbezogenen, vertraulichen oder anderweitig sensitiven Daten werden entsprechennd der relevanten Sicherheit-Richtlinien geschützt.

Vertrauliche Informationen müssen vertraulich behandelt werden. Mitarbeiter von DEMANDA werden in Bezug auf das Thema „Datenschutz“ informiert, geschult und verpflichten sie sich mit Eintritt in das Unternehmen zur Einhaltung der Datenschutzrichtline. Die Mitarbeiter erhalten einen entsprechenden Nachweis nach Absoliverung der Datenschutz-Schulung.

Alle produktiven Server werden in ISO 27001 zertifizierten Rechenzentren betrieben. Die Sicherheit der Anwendungen zur Verarbeitung von personenbezogenen, vertraulichen oder anderweitig sensitiven Daten wird regelmäßig überprüft. Dazu führen externe Unternehmen regelmäßige Validierungen des ISO 27001 Standards durch.

Die Verwaltung von Benutzerrechten erfolgt ausschließlich durch die Geschäftsführung.

2.2. INTEGRITÄT

2.2.1. Weitergabekontrolle:

DEMANDA gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Folgende Maßnahmen werden gesetzt:

DEMANDA gewährleistet die Verschlüsselung der Daten im Rahmen einer netzwerkübergreifenden Datenübertragung.

Zudem ist die Verschlüsselung der Daten zwischen Systemen von DEMANDA (Anwendungsserver, Datenbankserver, Fileserver) zu jedem Zeitpunkt gewährleistet.

2.2.2. Eingabekontrolle

Es kann überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert und entfernt worden sind. Folgende Maßnahmen werden gesetzt:

DEMANDA erlaubt nur autorisierten Personen im Rahmen ihrer Arbeitsaufgabe auf personenbezogene Daten zuzugreifen.

Es besteht ein striktes Berechtigungskonzept, dass die Eingabe, Änderung und Löschung von Daten nur für dafür festgelegte User-IDs erlaubt.

2.3. VERFÜGBARKEIT UND BELASTBARKEIT

2.3.1. Verfügbarkeitskontrolle:

DEMANDA gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und setzt folgende Maßnahmen:

DEMANDA verfügt über Backup-Prozesse und weitere Maßnahmen, um die Verfügbarkeit geschäftskritischer Systeme bei Bedarf kurzfristig wiederherstellen.

Notfallprozesse und -systeme werden regelmäßig getestet.

Firewalls oder andere Techniken der Netzwerksicherheit werden angewandt.

DEMANDA trägt dafür Sorge, dass aktualisierte Antivirus-Produkte und gegebenenfalls notwendige Security-Patches auf allen Systemen verfügbar sind.

Einzelne Löschfristen werden sowohl für Metadaten, sowie Logfiles eingehalten. Insbesondere personenbezogenen Daten die in Geschäftsprozessen anfallen werden automatisiert nach Abschluss (30 Tage Löschfrist) oder Ablehnung (7 Tage Löschfrist) gelöscht.

2.4. ZWECKGEBUNDENHEIT, ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

2.4.1. Auftragskontrolle:

DEMANDA gewährleistet, dass personenbezogene Daten, die im Auftrag von verantwortlichen Auftraggeben verarbeitet werden, nur entsprechend der Weisungen des Auftraggebers verarbeitet werden können. Es werden folgende Maßnahmen gesetzt:

DEMANDA verfügt über Kontrollen und Prozesse, um die Einhaltung der Vertragserfüllung zu überprüfen.

Kundeninformationen werden prinzipiell als „vertraulich“ eingestuft.

DEMANDA verfügt über eigene AGB und beinhaltet in diesen detailliert geregelt Verpflichungen zum „Datenschutz“ und „Geheimhaltung“.

Mitarbeiter von DEMANDA sind vertraglich verpflichtet die Vertraulichkeit aller sensiblen Informationen zu respektieren, einschließlich der Informationen über Geschäftsgeheimnisse von Kunden und Partnern von DEMANDA und erfolgt eine stetige Sensibiliserung/Schulung der Mitarbeiter.