Technische und organisatorische Sicherheitsmaßnahmen der CSA Group

Die CSA Group und ihre Tochtergesellschaften und verbundenen Unternehmen (gemeinsam „CSA Group“) bekennen sich zum Schutz Ihrer personenbezogenen Daten. Wir teilen diese nicht, verkaufen sie nicht oder greifen nicht darauf zu, sofern dies nicht der Erbringung der vertraglichen Dienste an Sie oder Zwecken dient, für die Sie Ihre Einwilligung erteilt haben.

Dieses Dokument fasst die Datensicherheitsrichtlinien und -praktiken zusammen, die wir im Rahmen unseres Sicherheitsprogramms umgesetzt haben. Die Begriffe „Datenverarbeitung“ und „Datenverarbeiter“ sind wie in der Datenschutz-Grundverordnung 2016/679 EU (DGSVO) definiert.

Schutz unserer physischen Räumlichkeiten und Datenverarbeitungseinrichtungen

Personenbezogene Daten befinden sich auf Servern in (von Datenverarbeitern verwendeten) Rechenzentren der Stufe Tier 1 oder höher oder in sicheren dedizierten Server-Räumen innerhalb der physischen Räumlichkeiten der CSA Group. Alle Datenverantwortlichen sowie die physischen Räumlichkeiten der CSA Group verfügen über Sicherheitskontrollen, die den Zutritt Unbefugter auf EDV-Anlagen mit personenbezogenen Daten verhindern. Dazu gehört der Einsatz von Folgendem:

- Festgelegte Sicherheitsbereiche.
- Zugangskontrollen für Mitarbeiter und Dritte.
- Alarmanlagen.
- Zutritt mit Transponderkarten und/oder biometrischer Authentifizierung.
- Videoüberwachung und/oder Zugangsprotokolle.
- Zugangsverfahren für Besucher.

Schutz unserer Systeme

Die CSA Group hat Maßnahmen eingerichtet, um ein Eindringen unbefugter Personen in seine EDV-Systeme zu verhindern und zu erkennen. Systemkontrollen umfassen den Einsatz von Folgendem:

- Zugangskontrollen werden durch Stellenverantwortlichkeiten und den Einsatz von Autorisierungsverfahren umgesetzt.
- Privilegierte Zugriffskontrollen für Administratoren, separat verwaltet.
- Zugangsprotokolle.
- Einsatz von Next-Generation-Firewalls und netzwerkbasierten Zugriffsbeschränkungen.
- Erkennung und Verhinderung von Malware an mehreren Punkten.
- Verwendung zentral verwalteter Identitäten, starker Kennwörter, Multi-Faktor-Authentifizierung und digitaler Zertifikate.

- Intrusionsüberwachung und Reaktion auf erkannte Sicherheitsverletzungen und andere sicherheits- oder betriebsrelevante Ereignisse.
- Überwachung der Einhaltung von Sicherheitsvorschriften und Schwachstellen-Scans.
- Aktualisierungen von System-Patches und Sicherheits-Software-Updates.
- Externe Bewertungen und Penetrationstests.

Schutz unserer Daten

Zugriff auf die oder Offenlegung der von der CSA Group kontrollierten oder verarbeiteten personenbezogenen Daten wird über Zugriffsautorisierungsregeln und/oder Verschlüsselung geschützt. Autorisierte Personen, die Zugriff auf Systeme mit personenbezogenen Daten haben, dürfen auf die Daten nur im gestatteten und im Rahmen ihrer Stellenverantwortlichkeiten gewährten Umfang zugreifen, und nur zur Leistung von Diensten oder Aufgaben, wie den betroffenen Personen gegenüber dargestellt. Soweit von der CSA Group kontrollierte personenbezogene Daten durch Dritte verarbeitet werden, muss der Zugriff auf personenbezogene Daten gleichwertigen Kontrollen unterliegen. Diese Kontrollen umfassen:

- Kontrollierter Zugriff auf personenbezogene Daten über rollenbasierte Regeln, eindeutige Anmeldedaten und das Prinzip der geringsten Rechte.
- Verwendung von Verschlüsselung mit starken Algorithmen während Übermittlung und im Ruhezustand.
- Systeme, die Zugriffsprotokolle für einen angemessenen Zeitraum aufbewahren.
- Schulungen zur Mitarbeitersensibilisierung und Richtlinien für Nutzung von und Zugriff auf personenbezogene/n Daten.
- Regelmäßige Überprüfung der Konten, Zugriffsrechte und Administrator-Aktivitäten.

Gewährleistung unserer Datenverfügbarkeit

Die CSA Group hat Maßnahmen umgesetzt, um zu gewährleisten, dass personenbezogene Daten vor unbeabsichtigtem/r Verlust oder Zerstörung durch mögliche Katastrophen bei unseren Datenverarbeitern geschützt sind. Dazu gehören:

- Anforderungen und Service-Vereinbarungen für Systemleistung, Verfügbarkeit, Redundanz, physisch getrennte Sicherungsspeicher und Wiederherstellung im Katastrophenfall, alle mit entsprechenden Sicherheitssystemen und Prozess-Kontrollen.
- Backup-Richtlinien und -verfahren, Pläne zur Wiederherstellung im Katastrophenfall und dazugehörige Tests.
- Überwachung der Anwendungssystem- und Netzwerkverfügbarkeit in Echtzeit.

Verwaltung unserer externen Datenverarbeiter

Die CSA Group bleibt für von Drittverarbeitern verarbeitete personenbezogene Daten verantwortlich und hat Sicherheitsmaßnahmen umgesetzt, um für diese Daten ein mindestens gleichwertiges Schutzniveau zu gewährleisten, das sie bei direkter Verarbeitung genießen

würden. Zusätzlich dazu, dass wir vom Datenverarbeiter die oben genannten Leistungen verlangen, leistet die CSA Group auch Folgendes:

- Due-Diligence-Prüfungen der Sicherheits- und Verfügbarkeitskontrollen des Datenverarbeiters, seiner Leistungsfähigkeit, seiner Finanzdaten und anderer Risiken.
- Einsicht in unabhängige Prüfungen oder Bewertungen des Datenverarbeiters.
- Gewährleistung eines rechtlichen Mechanismus, der es der CSA Group gestattet, personenbezogene Daten von Bewohnern der Europäischen Union an den Datenverarbeiter zu übertragen.
- Wir verlangen, dass Verträge und Vereinbarungen eindeutig formuliert sind, einschließlich spezifische Klauseln zur Nutzung und Trennung von Daten sowie einer Bestätigung, dass das Eigentum an den / die Kontrolle über die Daten ausschließlich bei der CSA Group verbleibt~~:~~
- Service-Level-Management und Einsatz von Verbindungs-Managern bei kritischen Datenverarbeitern.