ZUSAMMENFASSUNG DER ORGANISATORISCHEN UND TECHNISCHEN SICHERHEITSMASSNAHMEN

Dieses Dokument stellt eine Zusammenfassung der technischen und organisatorischen Sicherheitsmaßnahmen und -kontrollen dar, die durch Keyloop für Produkte und Dienstleistungen angewendet werden, um personenbezogene Daten zu schützen. Diese Maßnahmen und Kontrollen werden von Zeit zu Zeit aktualisiert. Definierte Begriffe haben ihre Bedeutung gemäß den Allgemeinen Geschäftsbedingungen von Keyloop und den geltenden Produktspezifikationen.

1 Die globale Sicherheitsorganisation von Keyloop

1.1 Keyloop beschäftigt Mitarbeiter, deren ausschließliche Aufgaben im Bereich des Datenschutzes bzw. der Datensicherheit liegen.

1.2 Keyloop verfügt über umfassende Datenschutzrichtlinien, deren Kenntnisnahme von allen Mitarbeitern und Mitarbeiterinnen bestätigt wurde und die regelmäßig überprüft werden.

1.3 Keyloop schult regelmäßig Personal zu Datenschutzmaßnahmen.

1.4 Zu den Aufgaben der Globalen Organisation für Datenschutz und -sicherheit von Keyloop gehören:

1.4.1 die Aufrechterhaltung der Wirksamkeit der Sicherheitsstrategie, Standards, Richtlinien, Praktiken, Verfahren und technischen Kontrollen von Keyloop für das Unternehmen, einschließlich der regelmäßigen Überprüfung von Richtlinien, Standards, Schulungen und Dokumentation;

1.4.2 die Verwaltung und Untersuchung von Datenschutzvorfällen oder verstößen gegen die Unternehmenssicherheit und die Benachrichtigung des Kunden innerhalb von 72 Stunden nach bestätigten Vorfällen in Bezug auf personenbezogene Daten oder anderweitig, wenn der Vorfall dem Kunden voraussichtlich Schaden zufügen wird;

1.4.3 Tests und Bewertung der Aspekte bezüglich Datenschutze und Datensicherheit von Technologien, Systemen und Anwendungen, die bei Keyloop verwendet werden;

1.4.4 die Pflege eines Reaktionsplans für Datenschutzvorfälle und angemessener Perimeterschutz für Netzwerke;

1.4.5 die Anwendung angemessener Mechanismen, um die sichere Kommunikation der Kundeninformationen zu garantieren;

1.4.6 die Autorisierung, Authentifizierung und Protokollierung aller Zugriffe auf Kundeninformationen (einschließlich und ohne Einschränkung die Verwendung eindeutiger Kennungen für Benutzer);

1.4.7 die Sicherung der Kundeninformationen gegen unbeabsichtigte Offenlegung von Informationen bei der Speicherung und der Übertragung;

1.4.8 die Entsorgung von Kundeninformationen unter Verwendung von in der Branche etablierten Datenvernichtungsmethoden und unter Beibehaltung der Vernichtungszertifikate;

1.4.9 Verhinderung der Sichtbarkeit von Kundeninformationen und Implementierung eines Modells mit geringster Berechtigung für den Zugriff auf Kundeninformationen;

1.4.10 administrative, technische und physische Sicherungen (einschließlich und ohne Einschränkung von Maßnahmen, die in den Gebäuden von Keyloop ergriffen werden), um Anlagen und Daten vor Verlusten, Missbrauch, unerlaubtem Zugriff, Offenlegung, Änderung und Zerstörung zu bewahren; und

1.4.11 zeitnahes Patchen und Behandeln von Schwachstellen, die beim Testen von Anwendungen festgestellt wurden.

2 Physische Zugriffskontrollen

2.1 Keyloop-Datenzentren verwenden physische Kontrollen einschließlich Zutrittskontrollmechanismen, kontrollierte Lieferungs- und Ladebereiche und Überwachung. Nur autorisiertes Personal hat Zutritt zu den Räumlichkeiten des Datenzentrums.

2.2 Die Geräte in den Keyloop-Datenzentren sind vor Stromausfällen und anderen Störungen geschützt, die durch Fehler bei unterstützenden Einrichtungen verursacht werden, und werden ordnungsgemäß gewartet.

2.3 Der Kunde ist verantwortlich für die physische Sicherheit der nicht-gehosteten Produkte und Dienstleistungen.

3 Systemzugriffskontrollen

3.1 Der Zugriff auf Kundendaten von Keyloop aus ist nur möglich für ermächtigte, authentifizierte Mitarbeiter, die den Zugriff für die Ausübung ihrer Funktion benötigen.

3.2 Die Keyloop-Maßnahmen beinhalten eindeutige Benutzer-IDs, Passwortstrategien mit regelmäßigen Passwortänderungen und Prozesse zur Entfernung von Zugriffsrechten für ausscheidendes Personal.

3.3 Die DMS-Software von Keyloop ermöglicht es den Kunden, Zugriffsparameter, Rollen und Berechtigungen zu verwalten.

4 Reaktion auf Datenschutzvorfälle

4.1 Die Globale Organisation für Datenschutz und -sicherheit von Keyloop pflegt einen detaillierten Reaktionsplan für Datenschutzvorfälle, der fortwährend überprüft und ggf. überarbeitet wird.