Datenschutzkonzept

Präambel

Die Firma Rocher Direktmarketing-Services ist seit 1992 im Bereich Fulfillmentdienstleistungen tätig. Neben den reinen Lager und Fullfilment Leistungen werden in immer stärkerem Maße web-basierte Fulfillmentlösungen angeboten. Da hierbei personenbezogenen Daten erhoben, verarbeitet und gespeichert werden unterliegt der Datenschutz der höchsten Priorität. Das vorliegende Konzept beschreibt, wie Datenschutz innerhalb der Firma berücksichtigt, umgesetzt und von allen Mitarbeitern gelebt wird.

Datenschutzpolitik und Verantwortlichkeiten im Unternehmen

Die Firma Rocher Direktmarketing-Services verpflichtet sich im Rahmen seiner gesellschaftlichen Verantwortung zur Einhaltung des gesetzlichen Datenschutzrechtes.

Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation der Rocher Direktmarketing-Services.

Wir definieren unsere eigenen Datenschutz-Ziele als Selbstverpflichtung. Dazu gehören:

- unbedingte Einhaltung der Vorgaben der EU-Datenschutz-Verordnung durch die gesamte Belegschaft
- unbedingte Einhaltung der unternehmenseigenen Datenschutzvorschriften durch die gesamte Belegschaft
- strikte Verpflichtung zur Geheimhaltung und Vertraulichkeit
- Datenschutzkonforme Arbeitsplatzgestaltung
- unbedingter Schutz vor Dateneinsicht durch Unbefugte

Rechtliche Rahmenbedingungen im Unternehmen

Das Erheben und Verarbeiten personenbezogener Daten ist in der Datenschutzgrund-verordnung (DS-GVO) geregelt. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (so genannter Betroffener). Generell gilt, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn gesetzliche Vorschriften dies ausdrücklich zulassen oder der Betroffene ausdrücklich eingewilligt hat. Die Einwilligung ist nur wirksam, wenn der Nutzer über die Tragweite des Verfahrens informiert wurde, dies heißt, welche Daten zu welchem Zweck in

welcher Form gespeichert und verarbeitet werden und die Einwilligung nicht in anderen Erklärungen versteckt worden ist.

Inhalt und Zweck des Konzeptes

Grundvoraussetzung für den Datenschutz ist die Datensparsamkeit. Daraus resultiert, dass nicht mehr Daten als benötigt verwendet werden. Als zweiten zentralen Punkt sehen wir die Notwendigkeit, Daten so früh als möglich zu pseudonymisieren bzw. zu anonymisieren.

Beschreibung der personenbezogenen Daten und Angabe der jeweiligen Zweckbindung (Nutzungszweck)

Kundendaten
Bei dem betroffenen Personenkreis handelt es sich um Kunden bzw. Mitarbeiter des Auftraggebers. Die Daten werden zu Zwecken der Abwicklung von Bestellaufträgen erhoben und gespeichert.

Verfahren zur Pseudonymisierung und Anonymisierung inklusive Risikoabschätzung

Die Verfahren zur Pseudonymisierung und Anonymisierung werden nach dem jeweils nach dem aktuellen Stand der Technik durchgeführt. Pseudonymisierung und Anonymisierung sind in der Regel immer dann notwendig, wenn keine gesetzliche Grundlage, die eine längere Speicherung als 91 Tage erfordert, existiert.

Verpflichtung zum Datenschutz

Die Geschäftsleitung eingeschlossen ihrer Mitarbeiter /-innen und Subunternehmer, verpflichten sich zur Einhaltung von datenschutzrechtlichen Vorschriften. Die betroffenen Personen haben eine entsprechende Datenschutzerklärung zur Geheimhaltungspflicht unterzeichnet.

Beschreibung der TOM´s zum Datenschutz

Die technischen und organisatorischen Maßnahmen zum Datenschutz werden hier nur in Stichworten aufgeführt und sind in einer eigenen Anlage TOM genauer definiert.

Vertraulichkeit

Zutrittskontrolle
Der Zugang zu den Räumlichkeiten ist nur autorisierten Personen möglich.

Zugangskontrolle
Der elektronische Zugang zu den Systemen ist durch Firewall-Technologien geschützt. Der Zugang ist nach heutigen technischen Standards mittels https und SSL-Verschlüsselung gesichert. Zugangsdaten zur Administration und Wartung der Firewall-Dienste sind Administratoren und verantwortlichen Mitarbeitern der Rocher Direktmarketing-Services bekannt. Die Passwörter werden regelmäßig geändert.

Zugriffskontrolle
Der Datenzugriff ist ausschließlich über unsere Softwarelösungen möglich und nach Mandanten getrennt. Die Mandantendaten sind logisch voneinander getrennt und verfügen jeweils über eine eigenständige Benutzer- und Zugriffsverwaltung für die Vergabe individueller Zugriffsberechtigungen. Auf Basis eines kundenspezifischen Rollenkonzepts werden Zugriffsberechtigungen definiert, damit personenbezogene Daten nach ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Weitergabekontrolle
Eine elektronische Weitergabe (Übertragung) von Daten erfolgt automatisiert mittels standardisierter Export-Schnittstellen innerhalb der Anwendungsumgebung. Der Zugriff auf Schnittstellen wird anwendungsseitig auf Basis der Berechtigungen gesteuert. Die Zugangskontrolle erfolgt anhand der eingesetzten technischen Komponenten.
Die Verfahren zur Übertragung an weitere Stellen (Dritte) werden anhand einer Schnittstellenspezifikation definiert und sind in der Ausführung durch den Auftraggeber steuerbar, die technischen Eigenschaften und Verfahren dann spezifisch in Abstimmung mit dem Auftraggeber definiert und innerhalb der Dokumentation berücksichtigt. In dieser Abhängigkeit sind ggfs. zusätzliche datenschutzrechtliche Regelungen mit Dritten zu vereinbarem.

Integrität

Eingabekontrolle
Anwendungsseitig ist gewährleistet, dass berechtigte Benutzer (i.d.R. Administratoren) nachträglich feststellen können, wann und von wem personenbezogene Daten erfasst, verändert oder entfernt worden sind. Die Dokumentation erfolgt zum Kundendatensatz und ist nicht manipulierbar.

Auftragskontrolle
Auf Basis der Datenschutzerklärung zur Auftragsdatenverarbeitung wird gewährleistet, dass die Verarbeitung von personenbezogenen Daten nur entsprechend den Weisungen des Vertragspartners (Nutzers) durchgeführt wird.

Verfügbarkeit

Verfügbarkeitskontrolle
Die Daten werden vom Auftragnehmer entsprechend dem dort vorliegenden Backup-Konzept gesichert.

Authentizität
Die Authentizität der Daten ergibt sich aus den in den verschiedenen Informationssystemen implementierten Verfahren, die eine Authentizität gewährleisten, zusammen mit den Organisationskonzepten unserer Firma:

- Berechtigungskonzept
- Sicherheitskonzept
- Protokollierungskonzept
- und das hier vorliegende Datenschutzkonzept.

Transparenz
Dem Transparenzgebot wird durch dieses Datenschutzkonzept genügt, in dem die Methoden der Erhebung und Nutzung der Daten beschrieben wird.

Trennungsgebot
Eine Trennung der Daten erfolgt nach Mandanten.