EVALANCHE
DATEN MANAGEMENT

ERHEBUNG, VERARBEITUNG UND LÖSCHUNG PERSONENBEZOGENER DATEN

EINFÜHRUNG 3

ADRESSPOOLS 4

EINWILLIGUNGSNACHWEISE 4

WERBEEINWILLIGUNG 4

TRACKING UND DATENERHEBUNG 5

ARTEN DER DATENERHEBUNG 5
EINSCHRÄNKUNG BEI PSEUDONYMISIERTEM TRACKING 5
COOKIE-VERGABE 5
TRACKING-DATEN 7
ANONYME TRACKING-HISTORIE 7
WIDERSPRUCHSMÖGLICHKEIT 7
ERHEBUNG VON IP-ADRESSEN BEI WEBFORMULARE 8
GEOKODIERUNG 8

DATENSCHUTZEINSTELLUNGEN 9

PRODUKTBEZOGENE BENACHRICHTIGUNGEN 9

PROTOKOLLIERUNG 10

CHANGE LOG 10
ADMIN LOG 10
LOGIN HISTORIE 11
WEBFORMULAR LOG 11
SERVER-/ERROR PROTOKOLLE 11

LÖSCHEN VON PERSONENBEZOGENEN DATEN 12

POOL (EMPFÄNGER) 12
SYSTEMBENUTZER 12
TRACKING 12
INFRASTRUKTUR UND BACKUP 12

DATENÜBERTAGUNG UND AUSKUNFT 13

EXTERNE DIENSTLEISTER 13

EINFÜHRUNG

Als professionellen Anbieter für E-Mail Marketing, Marketing Automation und Lead Management ist Datenschutz für uns ein zentrales Anliegen mit höchster Wertigkeit.

Die nachstehenden Informationen spiegeln unseren verantwortungsvollen Umgang mit personenbezogenen Daten wieder. Als Anbieter mit Sitz in Deutschland sind wir dem strengen deutschen und europäischen Datenschutz entsprechend der EU-DSGVO verpflichtet. Unser Umgang mit sensiblen Daten reflektiert die hohen gesetzlichen Anforderungen und geht vorausschauend teilweise über die aktuelle Rechtsprechung hinaus.

Unser Ziel ist, dass der Umgang mit Daten einheitlich, transparent, möglichst effizient und vor allem stets rechtskonform erfolgt. In diesem Dokument erläutern wir unser Vorgehen, mit dem wir vor allem auch unseren Kunden ermöglichen wollen, datenschutzrechtliche Anforderungen komfortabel umzusetzen.

Thematisch ist es untergliedert in

- Erhebung und Handhabung von Einwilligungsnachweisen,
- Tracking und Cookie Auswertung personenbezogener Daten,
- Handhabung von Protokollen,
- Aufbewahrung und Löschung personenbezogener Daten,
- Datenübertragung und Auskunft,
- Externe Dienstleister

ISO 27001

DIN EN ISO/IEC 27001:2022 zertifiziert

ADRESSPOOLS

Das System speichert marketingrelevanten Daten des Kunden (Adressdaten, Interessen, etc.) in sogenannten Pools. Hierbei handelt es sich um individuelle Datenstrukturen, die vom Kunden den Anforderungen entsprechend definiert werden können. Der Kunde ist somit für Inhalt und Struktur verantwortlich und übernimmt in der Regel Import und Löschung selbstständig. Eine automatisierte Löschung durch das System findet nicht statt, einzig nach Vertragsende den folgend beschriebenen zeitlichen Vorgaben entsprechend.

Die Speicherung der Daten dient dem Zweck der Veraltung marketingrelevanter Kundendaten und ist damit für die Erfüllung des Vertrags (Art. 6 (1) b) EU DSGVO) zwingend notwendig.

EINWILLIGUNGSNACHWEISE

WERBEEINWILLIGUNG

Um den Einwilligungs- und Austragungsnachweis rechtskonform abbilden zu können, werden bestimmte Daten standardmäßig erhoben, sofern der jeweilige Prozess über das System abgebildet wird.

Zu jedem Benutzerprofil, welches über ein Webformular per Double Opt-In Verfahren mittels bestätigter E-Mail-Adresse erzeugt wird, halten wir nachstehende Daten automatisch vor:

Eintragung/Änderung **(per Webformular)**	Eintragstyp (Neu oder Änderung) Datum und Uhrzeit IP-Adresse (optional)
Bestätigung **(per Link aus Double-Opt-in Aufforderung)**	Datum und Uhrzeit IP-Adresse (optional)
Austragung **(per Link aus eMailing, z.B. Newsletter)**	Datum und Uhrzeit IP-Adresse (optional) Austragungsstatus

Die Erhebung optionaler Daten kann im Rahmen der Datenschutzeinstellungen systemseitig aktiviert werden, siehe Datenschutzeinstellungen. Dies erfolgt mittels Vertragsanpassung.

Weitere Daten können individuell konfiguriert und zusätzlich gespeichert werden. Hierzu können Pool-Felder nach eigenen Wünschen ergänzt werden, z.B. für Einwilligungstexte und Zustimmungserklärungen. Alle weiteren Nachweise für die rechtskonforme Abbildung der Einwilligung müssen außerhalb des Systems abgebildet werden, z.B. inhaltliche Nachweise durch Screenshots der Anmeldeformulare und eMailings, etc.

Ein Anspruch auf Vollständigkeit besteht nicht. Bei Anwendungen im Ausland muss die landesspezifische Rechtslage hierfür durch den Kunden genauestens geprüft werden.

Die Speicherung der Daten dient dem Zweck des Einwilligungsnachweises und ist damit für die Erfüllung des Vertrags (Art. 6 (1) b) EU-DSGVO) zwingend notwendig.

TRACKING UND DATENERHEBUNG

Der Kunde entscheidet bei Vertragsabschluss oder –anpassung, ob die Datenerhebung im Rahmen des Trackings personenbezogen oder pseudonymisiert erfolgen soll. Abhängig von der im SaaS-Vertrag definierten Art der Datenerhebung wird eine Referenz zum korrespondierenden Profil gespeichert oder diese im Vorfeld zusätzlich pseudonymisiert. Eine nachträgliche Änderung des Verfahrens ist jederzeit schriftlich möglich. Die Konfiguration ist individuell pro Mandant des Kunden-Accounts einstellbar.

ARTEN DER DATENERHEBUNG

Die pseudonymisierte Datenspeicherung erfolgt unter Verwendung von Hashing, einer Methode die eine Zuordnung der erhobenen Informationen (Trackinginformationen und Cookies) zu einer bestimmbaren Person ausschließt. Die so gewonnenen Daten können lediglich für quantitative statistische Auswertungen verwendet werden. Personenbezogene Auswertungen und Datenexporte sind hierbei nicht möglich.

Bei personenbezogener Datenerhebung werden Trackingeinträge den entsprechenden Benutzerprofilen zugeordnet. Eine Auswertung aller Empfängeraktionen kann somit personenbezogen stattfinden. Die personenbezogene Datenerhebung und -auswertung sowie der Einsatz verschiedener Systemfunktionalitäten sind nur zulässig, soweit sich die Einwilligung des Betroffenen hierauf erstreckt. Hierfür trägt der Kunde die Verantwortung. Eine sorgfältige Prüfung ist anzuraten.

Die Speicherung der Daten dient dem Zweck statistischer Auswertungen und Bildung von Interessensprofilen (Tracking) und ist damit für die Erfüllung des Vertrags (Art. 6 (1) b) EU-DSGVO) notwendig.

EINSCHRÄNKUNG BEI PSEUDONYMISIERTEM TRACKING

Scoring, Live-Auswertungen von Profilaktivitäten, verschiedene Workflow-Bedingungen und Profile Tagging (Artikel) sind nur mit personenbezogener Datenerhebung möglich.

Die statistischen Auswertungen im System sind nahezu identisch (z.B. Versandstatistiken) bis auf die Export-Funktion der einzelnen aktionsauslösenden Profilen (Empfänger), die bei „anonymer" Erhebung bzw. pseudonymisierter Datenspeicherung nicht möglich ist. Die Profilhistorie zeigt in diesem Fall keine Aktionen des einzelnen Profils (Empfänger) und schließt eine nachträgliche Zusammenführung von personenbezogenen Informationen aus.

TRACKING VON E-MAIL-ÖFFNUNGEN

Die technische Erhebung finde durch ein 1x1 Pixel großes transparentes Bild (GIF) im Body der HTML-Variante der Mail statt. Der Bildname enthält die verschlüsselte Benutzer-ID, sofern personenbezogenes Tracking aktiv ist. Das Tracking ist alternativ pseudonymisiert durchführbar oder ganz deaktivierbar.

COOKIE-VERGABE

Innerhalb der Software kommen grundsätzlich nur unbedingt erforderliche und funktionale Cookies zum Einsatz, insbesondere zur Identifizierung des Nutzers und der Gewährleistung der Sicherheit sowie zur Umsetzung gewisser Voreinstellungen. Die Nutzung von Cookies (Typ 5) ist für die

Erbringung unserer Dienstleistungen und damit für die Erfüllung des Vertrags (Art. 6 (1) b) EU-DSGVO) zwingend erforderlich.

Des Weiteren können optionale Cookies zum Aufbau von Interessensprofilen und statistischen Auswertungen individuell aktiviert werden, siehe folgend Cookie Typ 1-4.

Cookie Typ	Einsatz/Bezeichnung	Name	Haltedauer Standardwerte
Typ 1	Tracking der Empfänger mittels unten genannten Objekten und Tracking-Daten	ewafut	24 Monate
Typ 2	Tracking (anonyme Historie), siehe anonyme Tracking-Historie	ewafutano	24 Monate
Typ 3	Übergabe von Conversioninformationen, siehe Tracking-Daten	mid <id-Gruppe> _<id-Kunde>	30 Tage
Typ 4 (alt)	Checkpoint (je Objekt), aktuell keine Neuanlage mehr möglich	T<id-Objekt> L<id-Link>	60 Tage
Typ 5	System-Coockie zur Identifizierung des Benutzer im Rahmen eines Session Managements	PHPSESSID	Beenden der Browsersitzung

Welche Objekte setzen Cookies, sofern das Setzen systemweit aktiviert ist?

Objekt	Erhebung Pseudonym.	Erhebung personenbez.
eMailing	(Typ 1 oder Typ 2) und Typ 3	(Typ 1 oder Typ 2) und Typ 3
LeadPage	(Typ 1 oder Typ 2) und Typ 3	(Typ 1 oder Typ 2) und Typ 3
Website	Typ 1 oder Typ 2	Typ 1 oder Typ 2
WebFormular	Typ 1 oder Typ 2	Typ 1 oder Typ 2
SmartLink	Typ 1 oder Typ 2	Typ 1 oder Typ 2
WebTouchPoint	Typ 1 oder Typ 2	Typ 1 oder Typ 2
Checkpoint (alt)	Keine	Typ 4 oder Typ 2

Abhängig von den verwendeten Objekten kann dies Auswirkung auf die Datenschutzerklärung der jeweiligen Webseite haben. Dies sollte genauestens geprüft werden.

TRACKING-DATEN

Folgende Daten werden im Rahmen des regulären Trackings der Objekte eMailing, LeadPage, Website, WebFormular, SmartLink und WebTouchPoint erhoben.

Tracking	• Datum und Uhrzeit • Typ (Objekt, z.B. eMailing, LeadPage,...) • Browser Referer • User Agent • Link-ID (optional) • Objekt-IDs • Optionale objektabhängige Informationen

Conversion Tracking	• Datum und Uhrzeit • Individuelle Übergabeparameter

Ebenso werden Cookies im Rahmen der kundenindividuellen Konfiguration mit einer Referenz des Empfängers gesetzt. Dies kann pseudonymisiert oder personenbezogen erfolgen, abhängig von den vertraglichen Einstellungen.

ANONYME TRACKING-HISTORIE

Die Erzeugung einer anonymen Tracking-Historie ist möglich jedoch standardmäßig deaktiviert. Dies muss in den Datenschutzeinstellungen durch den Anbieter im Vorfeld explizit aktiviert werden. Im Falle der Aktivierung wird eine anonyme Trackig-Historie mittels Cookies (Typ 2) erstellt und bei identifizierung des Empfängers automatisch konvertiert und zugeordnet (Datenschutzeinstellung: Anonyme Historie).

WIDERSPRUCHSMÖGLICHKEIT

Es wird eine personen-/profilbezogene Opt-out-/Widerspruchsmöglichkeit bzgl. der Erhebung und Auswertung von Tracking- und Cookie-Informationen unterstützt. Hierbei halten wir nachstehende Daten automatisch vor, sofern die Widerspruchsmöglichkeit per personalisiertem Link im eMailing oder Webformular verwendet wird. Ein Tacking-Widerspruch kann als Widerspruch oder invertiert als Zustimmung über Webformulare konfiguriert werden.

Tracking-Widerspruch	• Datum und Uhrzeit • Status • IP-Adresse (optional)

Eine statistische Auswertung der Empfängeraktionen findet daraufhin nicht mehr statt. Dies kann die Genauigkeit von Statistiken beeinflussen. Weitere Informationen zum Tracking und der Auswertung von Systemstatistiken finden sich in der Systemdokumentation.

Sofern gewünscht, besteht auch die Möglichkeit, Tracking und Cookie-Vergabe systemweit vollständig zu deaktivieren. Dies betrifft alle Objekte im Rahmen statistischer Auswertungen, wie z.B: eMailing, WebFormular, Smartlink, Checkpoint, WebTouchPoint, LeadPage, Website, Zielgruppenlink.

ERHEBUNG VON IP-ADRESSEN BEI WEBFORMULARE

Die Erhebung von IP-Adressen bei Webformularen aus dem System wird im SaaS-Vertrag definiert und bei initialer Einrichtung der Anwendung konfiguriert. Diese Konfiguration kann durch unseren Support nach entsprechender Beauftragung durch den Kunden jederzeit angepasst werden.

Wir weisen darauf hin, dass die Erhebung und Speicherung von IP-Adressen im Rahmen der Protokollierung von Einwilligungen datenschutzrechtlich zweifelhaft ist und daher ab 1.1.2016 nur noch erfolgt, sofern sie ausdrücklich vom Kunden beauftragt / angewiesen wurde.

Die erhobenen IP-Adressen sind in der Systemoberfläche einsehbar. Das System stellt die Informationen im Rahmen des Standarddatenexports für Profile zur Verfügung. Die individuelle Einrichtung einer kundeneigenen Exportfunktion ist per Webservices zusätzlich möglich.

Sofern die Speicherung von IP-Adressen deaktiviert wird hat dies Auswirkungen auf folgende Bereiche:

Werbeeinwilligung (Eintragung in WebFormular, Bestätigungs-Link aus eMailings, Abmelde-Link aus eMailings) und Protokolle (siehe Abschnitt Protokollierung).

Die Link-Tracking Funktionalität erhebt keine IP-Adressen.

GEOKODIERUNG

Das System bietet die Möglichkeit Adressangaben von Empfängern automatisch um Geokoordinaten (hausnummerninterpoliert) anzureichern, um Aktivitäten der Empfänger in Echtzeit geografisch auswerten zu können. Voraussetzung für eine Anreicherung ist die vertragliche Aktivierung der Funktion und vollständige Adressdatensätze der Empfänger (postalische Anschrift).

GEO-IP

Liegt keine vollständige postalische Anschrift vor und wird die Adresse über ein System-Web-Formular eingetragen, wird alternativ die IP-basierte Geokoordinate verwendet, die jedoch deutlich ungenauer ist.

Ein geographisch IP-basiertesTracking von Benutzeraktivitäten findet nicht statt. Die Geokoordinaten werden nur initial ermittelt und bei Adressänderung angepasst.

DATENSCHUTZEINSTELLUNGEN

Bei initialer Einrichtung des Systems für den jeweiligen Kunden/Mandanten können individuelle Datenschutzeinstellungen im Rahmen des SaaS-Vertrags definiert und konfiguriert werden.

Nach den EU-DSGVO Vorgaben für Privacy by Default, werden wir die Aktivierungen von folgenden Einstellungen ab dem 25.5.2018 nur nach vertraglicher Beauftragung vornehmen.

Einstellung	Standardwert	Konfiguration
Datenerhebung	s. Vertrag	Pseudonymisiert oder personenbezogen (durch Anbieter)
Tracking	s. Vertrag	Aktivierung oder Deaktivierung (durch Anbieter)
Cookies zu Trackingzwecken (Typ 1) (eMail, Formular, SmartLink, LeadPage, usw.)	s. Vertrag, 24 Monate	Aktivierung und Lebensdauer (durch Anbieter)
Anonyme Historie	s. Vertrag	Aktivierung oder Deaktivierung (durch Anbieter)
Cookies bei anonymer Historie (Typ 2)	deaktiviert, 24 Monate	Aktivierung und Lebensdauer (durch Anbieter)
Cookies zur Übermittlung von Conversion Informationen (Typ 3)	individuell, 30 Tage	Bei Conversion Tracking-Einstellungen im System
Erhebung IP-Adressen (Webformular-Aktionen)	s. Vertrag	Aktivierung oder Deaktivierung (durch Anbieter)

PRODUKTBEZOGENE BENACHRICHTIGUNGEN

Zur Erfüllung unserer vertraglichen Verpflichtungen im Hinblick auf die Benachrichtigung unserer Kunden zu wesentlichen Änderungen im Produkt, geplanten Wartungsarbeiten, technischen Problemen oder Ähnlichem behalten wir uns vor, die im Vertrag und der Registrierung benannten Personen direkt per E-Mail oder ggf. Telefon zu kontaktieren. Dies ist für die Erbringung unserer Support-Leistungen und damit für die Erfüllung des Vertrags (Art. 6 (1) b) EU-DSGVO) zwingend notwendig. Ein Widerspruchsrecht besteht nicht.

PROTOKOLLIERUNG

Mit jedem Zugriff auf das System werden automatisch allgemeine Protokolldaten, sogenannte Logs, erfasst. Ohne diese Daten wäre es technisch teilweise nicht möglich, die Inhalte der Software auszuliefern und darzustellen. Zudem ist die Verarbeitung dieser Daten aus Sicherheitsaspekten zwingend notwendig. Die Rechtsgrundlage hierfür findet sich in § 15 Abs. 1 Telemediengesetz (TMG) sowie Art. 6. (1) f EU-DSGVO. Ein Widerspruchsrecht besteht nicht.

Das System verwendet mehrere Arten der Protokollierung. Diese sind über die Benutzeroberfläche nicht einsehbar sowie änderbar und dienen lediglich zum Nachweis vertraglicher Pflichten und Änderungen personenbezogener Daten.

CHANGE LOG

Im ChangeLog werden Änderungen an Profildaten, durch WebFormular- und Profileditor-Aktionen, erfasst. Protokolliert werden:

Profiländerungen	• Datum und Uhrzeit
	• IP-Adresse (optional)
	• Profil-Referenz
	• E-Mail-Adresse
	• Eintragungstyp
	  ○ Ersteintragung
	  ○ Aktualisierung
	  ○ Einwilligungsnachweis

Die Speicherung erfolgt systemimmanent während der Vertragslaufzeit. Eine automatische Löschung während der Laufzeit ist nicht vorgesehen. Wichtige Protokolleinträge sind im System unter Profilhistorie des jeweiligen Profils ersichtlich.

ADMIN LOG

Das AdminLog protokolliert wichtige Aktionen von Systembenutzern. Protokolliert werden:

Benutzeraktionen (z.B. Initiierung Mailversand, Profillöschung,...)	• Aktion Benutzername und Vorname • Datum und Uhrzeit • IP-Adresse • Benutzeraktion • E-Mail-Adresse • Metadaten der Aktion

Die Speicherung erfolgt systemimmanent während der Vertragslaufzeit. Eine automatische Löschung während der Laufzeit ist nicht vorgesehen. Ein Zugriff auf die Protokolle ist durch Systembenutzer über die Systemoberfläche nicht möglich.

LOGIN HISTORIE

Die Login Historie protokolliert die Logins der Systembenutzer. Protokolliert werden:

Logins	• Benutzerreferenz Datum und Uhrzeit • IP-Adresse • UserAgent des Clients • Login Typ – Erfolg/Fehler

Eine automatische Löschung findet nach 6 Monaten statt. Die Protokolle können über die Benutzereinstellungen eingesehen werden.

WEBFORMULAR LOG

Im WebFormularLog werden Daten resultierend aus Webformularaktivitäten durch Webseitenbesucher oder E-Mail-Empfänger zu Nachweiszwecken (Permission) protokolliert.
Erhoben werden:

Webformular-Aktion (Eintragung, Profil Aktualisierung ..)	• Objekt- und Profilreferenz • E-Mail-Adresse • Datum und Uhrzeit • IP-Adresse (optional) • Aktionstyp (Eintragung, Aktualisierung, Permissionänderung) • Metadaten der Aktion

Die Einträge werden automatisch nach 12 Monaten oder bei Vertragsende gelöscht. Die Protokolle können über die WebFormular-Konfiguration eingesehen werden.

SERVER-/ERROR PROTOKOLLE

Im Rahmen der Protokollierung des Web- und E-Mail Traffics werden automatisch in folgenden Systemen externe IP-Adressen im Zusammenhang mit Benutzer- und Empfängeraktionen protokolliert. Dies ist notwendig, um die Sicherheit des Systems zu gewährleisten.

Infrastruktur (IDS, IPS, Webserver, Loadbalancer, Mail-Server, etc.)	• Datum und Uhrzeit • IP-Adresse • Aktion • URL • Browsertyp und Version • Referer • Betriebsystem

Ein Zugriff auf die Protokolle ist durch Systembenutzer über die Systemoberfläche nicht möglich.

LÖSCHEN VON PERSONENBEZOGENEN DATEN

Die nachstehend aufgeführten Regelungen gelten für die Löschung von personenbezogenen Daten sowie für Geo- und IP-Adressdaten im Produktivsystem (nicht Backup) und der System-Infrastruktur:

POOL (EMPFÄNGER)

Empfängerdaten von Kunden, ChangeLog, Geodaten (Koordinaten), Blacklist

Die manuelle Pflege/Löschung liegt in der Verantwortung des Kunden und kann selbständig erfolgen. Eine automatische Löschung erfolgt **4 Wochen nach Vertragsende**. Zwischenzeitlich werden die Daten gesperrt und vor unautorisiertem Zugriff geschützt. Sofern Daten für eigene Zwecke über diesen Zeitraum hinaus benötigt werden, müssen diese im Vorfeld exportiert werden.

Innerhalb des System von Benutzern initiierte automatische Backups, z.B. durch Import von Adressen oder Löschen von Zielgruppen, werden 30 Tage vorgehalten. Danach findet eine automatische Löschung statt.

SYSTEMBENUTZER

Benutzerzugänge von Kunden (Name, Vorname, eMail-Adresse, etc.):

Die manuelle Pflege/Löschung liegt in der Verantwortung des Kunden und kann selbständig erfolgen. Eine automatische Löschung erfolgt **4 Wochen nach Vertragsende**, es sei denn, dass diese zur Aufklärung oder zum Nachweis konkreter Rechtsverletzungen, die innerhalb der Aufbewahrungsfrist bekannt geworden sind, benötigt werden. Zwischenzeitlich werden die Daten gesperrt und vor unautorisiertem Zugriff geschützt.

TRACKING

Protokoll- und Tracking-Daten (AdminLog, Tracking, FormularLog):

Eine automatische Löschung **erfolgt 4 Wochen nach Vertragsende**, es sei denn, dass diese zur Aufklärung oder zum Nachweis konkreter Rechtsverletzungen, die innerhalb der Aufbewahrungsfrist bekannt geworden sind, benötigt werden. Zwischenzeitlich werden die Daten gesperrt und vor unautorisiertem Zugriff geschützt.

INFRASTRUKTUR UND BACKUP

Web- und Mailserver-Protokolle (IP-Adressen), Server Logfiles (Infrastruktur) auf Produktivsystem:

Löschung erfolgt automatisch **nach 7 Tagen** von den Produktivsystemen, es sei denn, dass diese zur Aufklärung oder zum Nachweis konkreter Rechtsverletzungen, die innerhalb der Aufbewahrungsfrist bekannt geworden sind, benötigt werden. Anschließend nur noch gesperrt und anonymisiert im Backup vorhanden.

Backup to Disc und auf Band: Löschung findet ca. nach 12 Monate nach Löschung aus den Produktivsystemen statt. Betroffene Datensätze werden für diesen Zeitraum als gesperrt markiert.

DATENÜBERTAGUNG UND AUSKUNFT

Die EU-DSGVO erlaubt die Speicherung personenbezogener Daten in strukturierter, maschinenlesbarer Form. Damit wahrt sie das Recht des Kunden, diese Daten auf ein anderes Unternehmen zu übertragen – etwa bei einem Anbieterwechsel.

Wir bieten hierfür die Möglichkeit per Reporting API alle gespeicherten personenbezogenen Daten der verwalteten Profile exportiern zu können. Sofern diese API in dem Kunden-Account aufgrund tariflicher Gründe nicht zur Verfügung steht, übernehmen wir ihm Rahmen des Supports den einmaligen Export.

Ebenso stellen wir einen Export einzelner Profile auf Anfrage bereit, um den Kunden bei Auskunftspflichten nach EU-DSGVO zu unterstützen. Das System wird derzeit erweitern, damit der Kunde dies eigenständig in Zukunft durchführen kann.

EXTERNE DIENSTLEISTER

Wir bieten verschiedene Mehrwertdienste in Zusammenarbeit mit externen Partnern/Dienstleistern an, siehe Auch Vertrag zur Auftragsverarbeitung. Abhängig von dem gebuchten Tarif stehen folgende Dienste externer Verarbeiter zur Verfügung.

Die Dienste können teils über entsprechende Konfigurationseinstellungen mithilfe der Rollen- und Rechtefunktionalitäten bzw. im Rahmen der vertraglichen Konfiguration aktiviert bzw. deaktiviert werden.

Dienst	Anbieter	Übermittlung personenbezogene Daten an Dienstleister	Serverstandort	deaktivierbar
Geocoding	Geofabrik GmbH	Postalische Adressen ohne Vor- und Nachnamen	Deutschland	ja
Auto. Adresskorrektur	Uniserv GmbH	Postalische Adressen ohne Vor- und Nachnamen	Deutschland	ja
Kartendienst	HERE Global B.V.	keine	EU	Ja
Social Media Push	Contentbird GmbH	Benutzername und E-Mail bei Setup	Deutschland	ja
E-Mailing Vorschau und SPAM-Check	Litmus Software Inc.	keine	USA	ja
Eyetracking (eMailing Inhalte)	Feng-GUI	keine	USA	ja
Vorlesefunktion	Read Speaker GmbH	keine	Schweden und USA	Ja
SMS Versand	LINK Mobility GmbH	Mobilfunk-Nummer, individuelle SMS Inhalte	Deutschland	Ja
Print Brief	Pin Digital GmbH	Nach Vereinbarung	Deutschland	Ja (Standard)
CRM-, CMS- und Shop-Konnektoren	Diverse (auf Anfrage)	Nach Vereinbarung	Diverse	ja (Standard)
Text- Bild und Kampagnengenerierung	OpenAI	keine	USA	ja

DATENSCHUTZ- UND INFORMATIONSSICHERHEITSBEAUFTRAGTER

Datenschutz- und Informationssicherheitsbeauftragter (ISB) der SC-Networks GmbH

Vasiliki Paschou und Jan Baumgärtner

activeMind AG - Management- und Technologieberatung

Potsdamer Straße 3 – 80802 München

Bei Fragen zu unserem Sicherheitskonzept und Datenschutz wenden Sie sich bitte an:
datenschutz@sc-networks.com

Siehe auch Dokument: SCN Bestellung DSB und SCN Bestellung ISB (Datenschutzpaket)