EVALANCHE
DATA MANAGEMENT

COLLECTION, PROCESSING AND DELETION OF PERSONAL DATA

Automatic translation from the German original

Responsible: Software Development
Confidentiality: public

Version: 28 from 04.05.2025

INTRODUCTION 3

ADDRESS POOLS 4

PROOF OF CONSENT 4

ADVERTISING CONSENT 4

TRACKING AND DATA COLLECTION 5

TYPES OF DATA COLLECTION 5
RESTRICTION FOR PSEUDONYMIZED TRACKING 5
COOKIE ALLOCATION 5
TRACKING DATA 7
ANONYMOUS TRACKING HISTORY 7
POSSIBILITY OF OBJECTION 7
COLLECTION OF IP ADDRESSES FOR WEB FORMS 8
GEOCODING 8

PRIVACY SETTINGS 9

PRODUCT RELATED NOTIFICATIONS 9

LOGGING 10

CHANGE LOG 10
ADMIN LOG 10
LOGIN HISTORY 11
WEBFORM LOG 11
SERVER/ERROR PROTOCOLS 11

DELETION OF PERSONAL DATA 12

POOL (RECEIVER) 12
SYSTEM USER 12
TRACKING 12
INFRASTRUCTURE AND BACKUP 12

DATA TRANSFER AND INFORMATION 13

EXTERNAL SERVICE PROVIDERS 13

INTRODUCTION

As a professional provider for email marketing, marketing automation and lead management, data protection is a central concern with the highest value for us.

The following information reflects our responsible handling of personal data. As a provider based in Germany, we are committed to strict German and European data protection in accordance with the EU-DSGVO. Our handling of sensitive data reflects the high legal requirements and, with foresight, in some cases goes beyond current case law.

Our goal is to ensure that data is handled uniformly, transparently, as efficiently as possible and, above all, always in compliance with the law. In this document, we explain our approach, with which we also want to enable our customers in particular to conveniently implement data protection requirements.

Thematically it is divided into

- Collection and handling of evidence of consent,
- Tracking and cookie evaluation of personal data,
- Handling protocols,
- Retention and deletion of personal data,
- Data transmission and information,
- External service providers

ISO 27001

DIN EN ISO/IEC 27001:2022 certified

ADDRESS POOLS

The system stores marketing-relevant data of the customer (address data, interests, etc.) in so-called pools. These are individual data structures that can be defined by the customer according to requirements. The customer is therefore responsible for the content and structure and usually handles import and deletion independently. An automated deletion by the system does not take place, only after the end of the contract according to the following time specifications.

The storage of the data serves the purpose of managing marketing-relevant customer data and is thus mandatory for the fulfillment of the contract (Art. 6 (1) b) EU DSGVO).

PROOF OF CONSENT

ADVERTISING CONSENT

In order to be able to map the consent and opt-out process in a legally compliant manner, certain data is collected by default, provided that the respective process is mapped via the system.

For each user profile, which is created via a web form by double opt-in procedure by means of confirmed e-mail address, we automatically keep the following data:

Entry/Change **(via web form)**	Entry type (New or Change) Date and time IP address (optional)
Confirmation **(via link from double opt-in request)**	Date and time IP address (optional)
Unsubscribe **(via link from emailing, e.g. newsletter)**	Date and time IP address (optional) Dispatch status

The collection of optional data can be activated on the system side as part of the data privacy settings, see Data privacy settings. This is done by means of contract adjustment.

Further data can be individually configured and additionally stored. For this purpose, pool fields can be supplemented according to own wishes, e.g. for consent texts and declarations of consent. All further evidence for the legally compliant mapping of consent must be mapped outside the system, e.g. proof of content through screenshots of the registration forms and emailings, etc.

There is no claim to completeness. For applications abroad, the country-specific legal situation must be checked in detail by the customer.

The storage of the data serves the purpose of the proof of consent and is thus mandatory for the fulfillment of the contract (Art. 6 (1) b) EU-DSGVO).

TRACKING AND DATA COLLECTION

The customer decides when concluding or adjusting the contract whether the data collection in the context of tracking is to be personalized or pseudonymized. Depending on the type of data collection defined in the SaaS contract, a reference to the corresponding profile is stored or this is additionally pseudonymized in advance. A subsequent change of the procedure is possible in writing at any time. The configuration can be set individually per client of the customer account.

TYPES OF DATA COLLECTION

The pseudonymized data storage is carried out using hashing, a method that excludes an assignment of the collected information (tracking information and cookies) to an identifiable person. The data obtained in this way can only be used for quantitative statistical evaluations. Personal evaluations and data exports are not possible.

In the case of personal data collection, tracking entries are assigned to the corresponding user profiles. An evaluation of all recipient actions can thus take place on a person-related basis. The personal data collection and evaluation as well as the use of various system functionalities are only permitted insofar as the consent of the person concerned extends to this. The customer is responsible for this. A careful examination is advisable.

The storage of the data serves the purpose of statistical evaluations and the formation of interest profiles (tracking) and is thus necessary for the fulfillment of the contract (Art. 6 (1) b) EU-DSGVO).

RESTRICTION WITH PSEUDONYMIZED TRACKING

Scoring, live evaluations of profile activities, various workflow conditions and profile tagging (articles) are only possible with personal data collection.

The statistical evaluations in the system are almost identical (e.g. dispatch statistics) except for the export function of the individual action-triggering profiles (recipients), which is not possible in the case of "anonymous" collection or pseudonymized data storage. In this case, the profile history does not show any actions of the individual profile (recipient) and excludes any subsequent merging of personal information.

EMAIL OPENINGS TRACKING

The technical collection takes place via a 1x1 pixel transparent image (GIF) in the body of the HTML variant of the mail. The image name contains the encrypted user ID if personal tracking is active. Alternatively, tracking can be pseudonymized or deactivated altogether.

COOKIE DISTRIBUTION

Within the software, only absolutely necessary and functional cookies are used as a matter of principle, in particular to identify the user and ensure security as well as to implement certain default settings. The use of cookies (type 5) is absolutely necessary for the provision of our services and thus for the fulfillment of the contract (Art. 6 (1) b) EU-DSGVO).

Furthermore, optional cookies can be individually activated to build up interest profiles and statistical evaluations, see following cookie type 1-4.

Cookie type	Application/Designation	Name	Holding period Standard values
Type 1	Tracking of recipients by means of objects and tracking data mentioned below	ewafut	24 months
Type 2	Tracking (anonymous history), see anonymous tracking history.	ewafutano	24 months
Type 3	Transfer of conversion information, see tracking data	mid < id group> _< id customer>	30 days
Type 4 (old)	Checkpoint (per object), currently no more new creation possible	T<id object> L<id link>	60 days
Type 5	System coockie for user identification in the context of session management	PHPSESSID	End the browser session

Which objects set cookies if setting is enabled system-wide?

Object	Collection pseudonym.	Collection persona.
eMailing	(Type 1 or Type 2) and Type 3	(Type 1 or Type 2) and Type 3
LeadPage	(Type 1 or Type 2) and Type 3	(Type 1 or Type 2) and Type 3
Website	Type 1 or Type 2	Type 1 or Type 2
WebForm	Type 1 or Type 2	Type 1 or Type 2
SmartLink	Type 1 or Type 2	Type 1 or Type 2
WebTouchPoint	Type 1 or Type 2	Type 1 or Type 2
Checkpoint (old)	None	Type 4 or Type 2

Depending on the objects used, this may have an impact on the privacy policy of the respective website. This should be checked carefully.

TRACKING DATA

The following data is collected as part of the regular tracking of the eMailing, LeadPage, Website, WebForm, SmartLink and WebTouchPoint objects.

Tracking	• Date and time • Type (object, e.g. eMailing, LeadPage,...) • Browser referrer • User Agent • Link ID (optional) • Object IDs • Optional object-dependent information

Conversion tracking	• Date and time • Individual transfer parameters

Likewise, cookies are set as part of the customer-specific configuration with a reference of the recipient. This can be pseudonymized or personalized, depending on the contractual settings.

ANONYMOUS TRACKING HISTORY

The generation of an anonymous tracking history is possible but deactivated by default. This must be explicitly activated in advance by the provider in the privacy settings. If activated, an anonymous tracking history is created using cookies (type 2) and automatically converted and assigned when the recipient is identified (privacy setting: Anonymous history).

POSSIBILITY OF OBJECTION

A personal/profile-related opt-out/objection option regarding the collection and evaluation of tracking and cookie information is supported. We automatically retain the following data if the opt-out option is used via a personalized link in the e-mailing or web form. A tacking objection can be configured as an objection or inverted as consent via web forms.

Tracking objection	• Date and time • Status • IP address (optional)

A statistical evaluation of the recipient actions then no longer takes place. This may affect the accuracy of statistics. For more information on tracking and evaluation of system statistics, see the system documentation.

If desired, it is also possible to completely deactivate tracking and cookie assignment system-wide. This applies to all objects within the scope of statistical evaluations, such as: eMailing, WebForm, Smartlink, Checkpoint, WebTouchPoint, LeadPage, Website, target group link.

COLLECTION OF IP ADDRESSES FOR WEB FORMS

The collection of IP addresses for web forms from the system is defined in the SaaS contract and configured during initial setup of the application. This configuration can be adjusted by our support at any time after appropriate assignment by the customer.

We would like to point out that the collection and storage of IP addresses as part of the logging of consents is dubious from a data protection point of view and will therefore only take place from 1.1.2016 if it has been expressly commissioned / instructed by the customer.

The collected IP addresses can be viewed in the system interface. The system provides the information as part of the standard data export for profiles. The individual setup of a customer-specific export function is additionally possible via web services.

If the storage of IP addresses is deactivated, this has an effect on the following areas:

Advertising consent (entry in WebForm, confirmation link from e-mailings, unsubscribe link from e-mailings) and logs (see Logging section).

The link tracking functionality does not collect IP addresses.

GEOCODING

The system offers the option of automatically enriching recipient address data with geocoordinates (house number interpolated) in order to be able to evaluate recipient activities geographically in real time. The prerequisite for enrichment is the contractual activation of the function and complete address data records of the recipients (postal address).

GEO-IP

If no complete postal address is available and the address is entered via a system web form, the IP-based geocoordinate is used as an alternative, but this is significantly less accurate.

Geographical IP-based tracking of user activities does not take place. The geocoordinates are only determined initially and adjusted if the address changes.

PRIVACY SETTINGS

When the system is initially set up for the respective customer/client, individual data protection settings can be defined and configured as part of the SaaS contract.

According to the EU-DSGVO requirements for Privacy by Default, we will perform the activations of the following settings from 25.5.2018 only after contractual assignment.

Setting	Default value	Configuration
Data collection	s. Contract	Pseudonymized or personalized (by provider)
Tracking	s. Contract	Activation or deactivation (by provider)
Cookies for tracking purposes (type 1) (eMail, form, SmartLink, LeadPage, etc.)	s. Contract, 24 months	Activation and lifetime (by provider)
Anonymous history	s. Contract	Activation or deactivation (by provider)
Cookies with anonymous history (type 2)	deactivated, 24 months	Activation and lifetime (by provider)
Cookies for the transmission of conversion information (type 3)	individual, 30 days	For conversion tracking settings in the system
Collection of IP addresses (web form actions)	s. Contract	Activation or deactivation (by provider)

PRODUCT RELATED NOTIFICATIONS

In order to fulfill our contractual obligations with regard to notifying our customers of significant changes in the product, planned maintenance work, technical problems or similar, we reserve the right to contact the persons named in the contract and the registration directly by e-mail or telephone, if necessary. This is absolutely necessary for the provision of our support services and thus for the fulfillment of the contract (Art. 6 (1) b) EU-DSGVO). There is no right of objection.

LOGGING

With each access to the system, general log data, so-called logs, are automatically collected. Without this data, it would not be technically possible to deliver and display the contents of the software. In addition, the processing of this data is mandatory for security reasons. The legal basis for this is found in Section 15 (1) of the German Telemedia Act (TMG) as well as Art. 6. (1) f EU-DSGVO. There is no right to object.

The system uses several types of logging. These cannot be viewed or changed via the user interface and are only used to prove contractual obligations and changes to personal data.

CHANGE LOG

The ChangeLog records changes to profile data, through WebForm and Profile Editor actions. The following are logged:

Profile changes	• Date and time • IP address (optional) • Profile Reference • E-mail address • Entry type ○ Initial registration ○ Update ○ Proof of consent

The storage is inherent in the system during the term of the contract. Automatic deletion during the term is not provided for. Important log entries are visible in the system under profile history of the respective profile.

ADMIN LOG

The AdminLog logs important actions of system users. The following are logged:

User actions **(e.g. initiation mail dispatch, profile deletion,...)**	• Action username and first name • Date and time • IP address • User action • E-mail address • Action metadata

The storage is inherent in the system during the term of the contract. There is no provision for automatic deletion during the term of the contract. System users cannot access the logs via the system interface.

LOGIN HISTORY

The login history logs the logins of the system users. Logged are:

Logins	• User reference date and time • IP address • UserAgent of the client • Login type - success/error

An automatic deletion takes place after 6 months. The logs can be viewed via the user settings.

WEBFORM LOG

In WebFormLog, data resulting from web form activities by website visitors or email recipients are logged for verification purposes (permission). Data collected:

Web form action (registration, profile update ..)	• Object and profile reference • E-mail address • Date and time • IP address (optional) • Action type (entry, update, permission change) • Action metadata

The entries are automatically deleted after 12 months or at the end of the contract. The logs can be viewed
via the WebForm configuration.

SERVER/ERROR PROTOCOLS

As part of the logging of web and e-mail traffic, external IP addresses are automatically logged in the following systems in connection with user and recipient actions. This is necessary to ensure the security of the system.

Infrastructure (IDS, IPS, web server, load balancer, mail server, etc.)	• Date and time • IP address • Action • URL • Browser type and version • Referrer • Operating system

Access to the logs is not possible by system users via the system interface.

DELETION OF PERSONAL DATA

The regulations listed below apply to the deletion of personal data as well as geo and IP address data in the productive system (not backup) and the system infrastructure:

POOL (RECEIVER)

Recipient data of customers, ChangeLog, geodata (coordinates), blacklist

Manual maintenance/deletion is the responsibility of the customer and can be done independently. Automatic deletion takes place **4 weeks after the end of the contract**. In the meantime, the data is blocked and protected against unauthorized access. If data is required for own purposes beyond this period, it must be exported in advance.

Automatic backups initiated by users within the system, e.g. by importing addresses or deleting target groups, are retained for 30 days. After that, an automatic deletion takes place.

SYSTEM USER

User accesses of customers (name, first name, eMail address, etc.):

Manual maintenance/deletion is the responsibility of the customer and can be done independently. Automatic deletion takes place **4 weeks after the end of the contract, unless this** is required for clarification or proof of specific legal violations that have become known within the retention period. In the meantime, the data will be blocked and protected from unauthorized access.

TRACKING

Log and tracking data (AdminLog, Tracking, FormLog):

Automatic deletion **takes place 4 weeks after the end of the contract, unless this** is required for clarification or proof of specific legal violations that have become known within the retention period. In the meantime, the data will be blocked and protected from unauthorized access.

INFRASTRUCTURE AND BACKUP

Web and mail server logs (IP addresses), server log files (infrastructure) on production system:

Deletion takes place automatically **after 7 days** from the productive systems, unless they are required for clarification or proof of specific legal violations that have become known within the retention period. Afterwards only locked and anonymized available in the backup.

Backup to Disc and to Tape: Deletion takes place approximately 12 months after deletion from production systems. Affected records are marked as locked for this period.

DATA TRANSFER AND INFORMATION

The EU GDPR allows personal data to be stored in structured, machine-readable form. It thus preserves the customer's right to transfer this data to another company - for example, when changing providers.

We offer the possibility to export all stored personal data of the managed profiles via Reporting API. If this API is not available in the customer account due to tariff reasons, we will take over the one-time export as part of the support.

Likewise, we provide an export of individual profiles on request to support the customer with information obligations according to EU-DSGVO. The system is currently being expanded so that the customer can do this independently in the future.

EXTERNAL SERVICE PROVIDERS

We offer various value-added services in cooperation with external partners/service providers, see also contract for order processing. Depending on the booked tariff, the following services of external processors are available.

The services can be activated or deactivated in part via corresponding configuration settings using the role and rights functionalities or as part of the contractual configuration.

Service	Provider	Transferred personal. Data to service provider	Server location	deactivatable
Geocoding	Geofactory Ltd.	Postal addresses without first and last names	Germany	yes
Auto. Address correction	Uniserv GmbH	Postal addresses without first and last names	Germany	yes
Map service	HERE Global B.V.	none	EU	yes
Social media push	Contentbird GmbH	Username and email at setup	Germany	yes
Emailing preview and SPAM check	Litmus Software Inc.	none	USA	yes
Read aloud function	Read Speaker Ltd.	none	Sweden and USA	yes
SMS dispatch	LINK Mobility GmbH	Mobile number, individual SMS contents	Germany	yes
Print letter	Pin Digital Ltd.	By arrangement	Germany	yes (default)
CRM, CMS and store connectors	Various (on request)	By arrangement	Various	yes (default)
Text- Bild und Kampagnengenerierung	OpenAI	keine	USA	yes

DATA PROTECTION AND INFORMATION SECURITY OFFICER

Data Protection and Information Security Officer (ISB) of SC-Networks GmbH

Vasiliki Paschou und Jan Baumgärtner

activeMind AG - Management and Technology Consulting

Potsdamer Street 3 - 80802 Munich

For questions regarding our security concept and data protection, please contact:
datenschutz@sc-networks.com