



EVALANCHE DATA MANAGEMENT

COLLECTION, PROCESSING, AND DELETION OF PERSONAL
DATA



INTRODUCTION	3
ADDRESS POOLS	4
EVIDENCE OF CONSENT	4
MARKETING CONSENT	4
TRACKING AND DATA COLLECTION	4
TYPES OF DATA COLLECTION.....	5
RESTRICTIONS ON PSEUDONYMIZED TRACKING	5
TRACKING OF EMAIL OPENS	5
COOKIE ASSIGNMENT.....	5
TRACKING DATA.....	7
ANONYMOUS TRACKING HISTORY	7
OPTION TO OBJECT	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
WEB FORM LOG	11
SERVER/ERROR LOGS.....	11
DELETION OF PERSONAL DATA	12
POOL (RECIPIENTS).....	12
SYSTEM USERS	12
TRACKING	12
INFRASTRUCTURE AND BACKUP.....	12
DATA PORTABILITY AND ACCESS TO DATA	13
EXTERNAL SERVICE PROVIDERS	13
DATA PROTECTION AND INFORMATION SECURITY OFFICER	14



INTRODUCTION

As a professional provider of email marketing, marketing automation, and lead management, data protection is a central concern of the utmost importance to us.

The information below reflects our responsible handling of personal data. As a provider based in Germany, we are bound by strict German and European data protection laws in accordance with the EU GDPR. Our handling of sensitive data reflects the high legal requirements and, in some cases, proactively goes beyond current case law.

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

It is organized thematically into

- collection and handling of consent records,
- Tracking and cookie analysis of personal data,
- Handling of logs,
- Retention and deletion of personal data,
- Data transfer and access requests,
- External Service Providers

ISO 27001

DIN EN ISO/IEC 27001:2022 certified



ADDRESS POOLS

The system stores the customer's marketing-related data (address information, interests, etc.) in so-called pools. These are individual data structures that can be defined by the customer according to their requirements. The customer is therefore responsible for the content and structure and generally handles the import and deletion independently. The system does not perform automated deletion; deletion occurs only upon termination of the contract in accordance with the timeframes described below.

The storage of this data serves the purpose of managing marketing-related customer data and is therefore strictly necessary for the performance of the contract (Art. 6(1)(b) EU GDPR).

EVIDENCE OF CONSENT

MARKETING CONSENT

To document consent and opt-out records in compliance with the law, certain data is collected by default, provided that the respective process is handled through the system.

For each user profile created via a web form using the double opt-in procedure with a confirmed email address, we automatically retain the following data:

Registration/Change (via web form)	Registration Type (New or Update) Date and time IP address (optional)
Confirmation (via link from double opt-in request)	Date and time IP address (optional)
Unsubscribe (via a link in an email, e.g., newsletter)	Date and time IP address (optional) Unsubscribe status

The collection of optional data can be enabled in the system's privacy settings; see Privacy Settings. This is done by modifying the contract.

Additional data can be individually configured and stored. For this purpose, pool fields can be customized as desired, e.g., for consent texts and declarations of consent. All other evidence required to demonstrate legally compliant consent must be maintained outside the system, e.g., evidence of content via screenshots of registration forms and email campaigns, etc.

This list is not exhaustive. For applications outside Germany, the customer must carefully review the country-specific legal situation.

The storage of this data serves as proof of consent and is therefore strictly necessary for the performance of the contract (Art. 6(1)(b) of the EU GDPR).

TRACKING AND DATA COLLECTION

Upon conclusion or amendment of the contract, the customer decides whether data collection for tracking purposes should be performed on a personal or pseudonymized basis. Depending on the



type of data collection defined in the SaaS contract, a reference to the corresponding profile is stored, or the profile is additionally pseudonymized in advance. A subsequent change to this procedure may be made in writing at any time. The configuration can be customized individually for each tenant of the customer's account.

TYPES OF DATA COLLECTION

Pseudonymized data storage is performed using hashing, a method that prevents the collected information (tracking information and cookies) from being linked to an identifiable individual. The data obtained in this way may only be used for quantitative statistical analyses. Personalized analyses and data exports are not possible in this context.

In the case of personal data collection, tracking entries are assigned to the corresponding user profiles. An analysis of all recipient actions can thus be performed on a personal basis. The collection and analysis of personal data, as well as the use of various system functionalities, are only permitted to the extent that the data subject's consent covers these activities. The customer bears responsibility for this. A careful review is recommended.

The storage of data serves the purpose of statistical analysis and the creation of interest profiles (tracking) and is therefore necessary for the performance of the contract (Art. 6(1)(b) EU GDPR).

RESTRICTIONS ON PSEUDONYMIZED TRACKING

Scoring, real-time analysis of profile activities, various workflow conditions, and profile tagging (articles) are only possible with the collection of personal data.

The statistical analyses in the system are nearly identical (e.g., mailing statistics) except for the export function for individual action-triggering profiles (recipients), which is not possible with "anonymous" collection or pseudonymized data storage. In this case, the profile history does not show any actions taken by the individual profile (recipient) and precludes any subsequent merging of personally identifiable information.

TRACKING OF EMAIL OPENS

Technical collection takes place via a 1x1-pixel transparent image (GIF) in the body of the HTML version of the email. The image name contains the encrypted user ID, provided that personal tracking is active. Alternatively, tracking can be performed in a pseudonymized manner or disabled entirely.

COOKIE ASSIGNMENT

The software generally uses only strictly necessary and functional cookies, in particular to identify the user, ensure security, and implement certain default settings. The use of cookies (Type 5) is strictly necessary for the provision of our services and thus for the performance of the contract (Art. 6(1)(b) EU GDPR).

Furthermore, optional cookies for creating interest profiles and statistical analyses can be enabled on an individual basis; see Cookie Types 1–4 below.

Cookie Type	Purpose/Description	Name	Retention Period Default Values
--------------------	----------------------------	-------------	--



Type 1	Tracking of recipients using the objects and tracking data listed 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 (legacy)	Checkpoint (per object), currently cannot be created anymore	T<object-id> L<link-id>	60 days
Type 5	System cookie used to identify the user as part of session management	PHPSESSID	End of browser session

Which objects set cookies, provided that cookie setting is enabled system-wide?

Object	Collection: Pseudonymous.	Collection Personal
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
Web form	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 affect the privacy policy of the respective website. This should be carefully reviewed.



TRACKING DATA

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

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

Conversion Tracking	• Date and time • Custom transfer parameters
---------------------	--

Cookies are also set as part of the customer-specific configuration with a reference to the recipient. This can be done pseudonymously or on a personally identifiable basis, depending on the contractual settings.

ANONYMOUS TRACKING HISTORY

The creation of an anonymous tracking history is possible but is disabled by default. This must be explicitly enabled in advance by the provider in the privacy settings. If enabled, an anonymous tracking history is created using cookies (Type 2) and is automatically converted and assigned upon identification of the recipient (privacy setting: Anonymous History).

OPTION TO OBJECT

A person- or profile-based opt-out option regarding the collection and analysis of tracking and cookie information is supported. In this context, we automatically retain the following data provided that the opt-out option is used via a personalized link in an email or web form. A tracking opt-out can be configured as an opt-out or, conversely, as consent via web forms.

Tracking Objection	• Date and Time • Status • IP address (optional)
--------------------	--

Statistical analysis of recipient actions will no longer take place. This may affect the accuracy of statistics. Further information on tracking and the analysis of system statistics can be found in the system documentation.



If desired, you can also completely disable tracking and cookie assignment system-wide. This applies to all objects used in statistical analyses, such as: eMailing, WebFormular, Smartlink, Checkpoint, WebTouchPoint, LeadPage, Website, , and Target Group Link.

COLLECTION OF IP ADDRESSES FOR WEB FORMS

The collection of IP addresses from web forms within the system is defined in the SaaS agreement and configured during the initial setup of the application. This configuration can be adjusted at any time by our support team upon request from the customer.

Please note that the collection and storage of IP addresses as part of consent logging is questionable under data protection law and, as of January 1, 2016, will therefore only take place if expressly requested or instructed by the customer.

The collected IP addresses can be viewed in the system interface. The system makes this information available as part of the standard data export for profiles. It is also possible to set up a custom export function for the customer via web services.

If the storage of IP addresses is disabled, this will affect the following areas:

Advertising consent (entry in web forms, confirmation links in email campaigns, unsubscribe links in email campaigns) and logs (see the "Logging" section).

The link-tracking functionality does not collect IP addresses.

GEOCODING

The system offers the ability to automatically enrich recipients' address information with geographic coordinates (interpolated based on house numbers) in order to geographically analyze recipients' activities in real time. Prerequisites for this enrichment are the contractual activation of the feature and complete address records for the recipients (mailing address).

GEO-IP

If a complete mailing address is not available and the address is entered via a system web form, the IP-based geographic coordinate is used as an alternative; however, this is significantly less accurate.

There is no geographically IP-based tracking of user activities. The geocoordinates are determined only initially and adjusted in the event of an address change.



PRIVACY SETTINGS

During the initial setup of the system for the respective customer/client, individual privacy settings can be defined and configured as part of the SaaS agreement.

In accordance with the EU GDPR requirements for "Privacy by Default," we will only activate the following settings as of May 25, 2018, upon contractual request.

Setting	Default Value	Configuration
Data Collection	See contract	Pseudonymized or personally identifiable (by provider)
Tracking	See contract	Enabling or disabling (by provider)
Cookies for tracking purposes (Type 1) (email, form, SmartLink, LeadPage, etc.)	See contract, 24 months	Activation and lifespan (by provider)
Anonymous history	See contract	Activation or deactivation (by provider)
Cookies for anonymous history (Type 2)	Disabled, 24 months	Enabling and Lifespan (by provider)
Cookies for transmitting conversion information (Type 3)	Varies, 30 days	When conversion tracking is enabled in the system
Collection of IP addresses (web form actions)	See contract	Activation or deactivation (by provider)

PRODUCT-RELATED NOTIFICATIONS

To fulfill our contractual obligations regarding the notification of our customers about significant changes to the product, scheduled maintenance, technical issues, or similar matters, we reserve the right to contact the individuals named in the contract and during registration directly via email or, if necessary, by phone. This is strictly necessary for the provision of our support services and thus for the fulfillment of the contract (Art. 6 (1) b) EU GDPR). There is no right to object.



LOGGING

Every time the system is accessed, general log data is automatically collected. Without this data, it would in some cases be technically impossible to deliver and display the software's content. Furthermore, the processing of this data is absolutely necessary for security reasons. The legal basis for this is found in Section 15(1) of the German Telemedia Act (TMG) and Article 6(1)(f) of the EU GDPR. There is no right to object.

The system uses several types of logging. These cannot be viewed or modified via the user interface and serve solely to document contractual obligations and changes to personal data.

CHANGE LOG

The ChangeLog records changes to profile data resulting from WebFormular and Profile Editor actions. The following are logged:

Profile changes	• Date and time • IP address (optional) • Profile reference • Email address • Registration Type ○ Initial entry ○ Update ○ Proof of Consent
------------------------	--

Data is stored within the system for the duration of the contract. Automatic deletion during the contract term is not provided for. Important log entries can be viewed in the system under "Profile History" for the respective profile.

ADMIN LOG

The Admin Log records important actions performed by system users. The following are logged:

User actions (e.g., initiating email sending, profile deletion, etc.)	• Action Username and first name • Date and time • IP address • User action • Email address • Action metadata
---	---

Data is stored within the system for the duration of the contract. Automatic deletion during the contract term is not provided for. System users cannot access the logs via the system interface.



LOGIN HISTORY

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

Logins	• User ID • Date and time • IP address • Client User-Agent • Login Type – Success/Failure
---------------	---

Data is automatically deleted after 6 months. The logs can be viewed in the user settings.

WEB FORM LOG

The Web Form Log records data resulting from web form activities by website visitors or email recipients for verification purposes (permission). The following data is collected:

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

Entries are automatically deleted after 12 months or upon contract expiration. The logs can be viewed via the WebForm configuration.

SERVER/ERROR LOGS

As part of the logging of web and email traffic, external IP addresses associated with user and recipient actions are automatically logged in the following systems. 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
--	--

System users cannot access the logs via the system interface.



DELETION OF PERSONAL DATA

The provisions listed below apply to the deletion of personal data as well as geolocation and IP address data in the production system (not the backup) and the system infrastructure:

POOL (RECIPIENTS)

Customer recipient data, ChangeLog, geodata (coordinates), blacklist

Manual maintenance/deletion is the responsibility of the customer and can be performed independently. Automatic deletion occurs **4 weeks after the end of the contract**. In the meantime, the data is locked and protected against unauthorized access. If data is needed for the customer's own purposes beyond this period, it must be exported in advance.

Automatic backups initiated by users within the system—for example, by importing addresses or deleting target groups—are retained for 30 days. After that, they are automatically deleted.

SYSTEM USERS

Customer user accounts (last name, first name, email address, etc.):

Manual maintenance/deletion is the customer's responsibility and can be performed independently. Automatic deletion occurs **4 weeks after the end of the contract**, unless the data is needed to investigate or provide evidence of specific legal violations that became known within the retention period. In the meantime, the data is locked and protected from unauthorized access.

TRACKING

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

Automatic deletion **occurs 4 weeks after the end of the contract**, unless the data is needed to investigate or provide evidence of specific legal violations that became known during the retention period. In the meantime, the data is locked and protected from unauthorized access.

INFRASTRUCTURE AND BACKUP

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

System logs containing personal data are automatically deleted from the servers after 7 days, unless they are needed to investigate or provide evidence of specific legal violations that became known within the retention period.

Exceptions include log data containing other items listed here (admin log, login history, etc.), as well as core application functions (email delivery: 4 weeks).

Logs are stored in anonymized form for up to 12 months.

Backups to disk and tape: Deletion occurs approximately 12 months after deletion from the production systems. Affected data records are marked as locked for this period.



DATA PORTABILITY AND ACCESS TO DATA

The EU GDPR permits the storage of personal data in a structured, machine-readable format. This safeguards the customer's right to transfer this data to another company—for example, when switching providers.

To this end, we offer the option to export all stored personal data from managed profiles via the Reporting API. If this API is not available in the customer's account due to pricing plan restrictions, we will perform a one-time export as part of our support services.

We also provide the option to export individual profiles upon request to assist customers in fulfilling their obligations to provide information under the EU GDPR. We are currently expanding the system so that customers can perform this task independently in the future.

EXTERNAL SERVICE PROVIDERS

We offer various value-added services in collaboration with external partners/service providers; see also the Data Processing Agreement. Depending on the selected plan, the following services from external processors are available.

Some of these services can be enabled or disabled via the appropriate configuration settings using the roles and permissions features or as part of the contractual configuration.

Service	Provider	Transfer of Personal Data to Service Providers	Server Location	Can be disabled
Geocoding	Geofabrik GmbH	Postal addresses without first and last names	Germany	Yes
Automatic 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 during setup	Germany	Yes
Email Preview and SPAM Check	Litmus Software Inc.	None	USA	Yes
Read-Aloud Feature	Read Speaker GmbH	None	Sweden and the USA	Yes
SMS Sending	LINK Mobility GmbH	Cell phone number, custom SMS content	Germany	Yes
Print Letter	Pin Digital GmbH	By appointment	Germany	Yes (Standard)
CRM, CMS, and e-commerce connectors	Various (upon request)	By arrangement	Various	Yes (Standard)
Text, image, and campaign generation	OpenAI	None	USA	Yes



DATA PROTECTION AND INFORMATION SECURITY OFFICER

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

Vasiliki Paschou and Jan Baumgärtner

activeMind AG - Management and Technology Consulting

Potsdamer Straße 3 – 80802 Munich

If you have any questions regarding our security policy and data protection, please contact:

datenschutz@sc-networks.com

See also the document: **SCN Order DSB** and **SCN Order ISB (Data Protection Package)**