PRIVACY POLICY AS SUPPORT B.V.

Versie 1.6

Frankenstraat 77,
6582 CW Heumen
KVK 09122754
www.assupport.nl

Privacy policy AS Support

Introduction

AS Support B.V. respects the privacy of its customers and the end users of its services. In this privacy policy, we explain how we handle personal data, which data we process, and how we comply with the General Data Protection Regulation (GDPR).

What Data Do We Process?

AS Support processes personal data necessary for our services, such as:

1. **Contact details:** Name, address, email address, phone number.
2. **Financial data:** Information required for invoicing or for arranging mortgages or insurance.
3. **Technical data:** IP addresses, browser details, and log files.
4. **Sensitive data:** Financial information entered into tools or modules.
5. **Data from connected third-party platforms:** Data obtained through integrations activated by the customer, such as Google Drive and Google Sheets, including selected spreadsheet content, file metadata, account identifiers, and encrypted authorization credentials, insofar as necessary to provide the requested integration functionality.

Social Media Integration

Our service offers optional integrations with social media platforms to publish news articles on your behalf. These integrations are only active when you choose to enable them yourself.

Socials Hub (Facebook Integration)

If you use the Socials Hub module (as registered with Meta) to publish news articles to Facebook, the following additional data is processed:

- **Facebook page IDs and access tokens** (stored in encrypted form only).
- **Name, email address, and (if relevant) profile information** of the account linked to the Facebook page, only as far as necessary for posting messages on your behalf.
- **News posts** published on Facebook via our service, including related metadata (publish time, post ID, etc.).

This data is used solely to publish news articles to your own Facebook page on your behalf and to manage your Facebook connection. We do not share data with Facebook except as strictly necessary for this functionality. You can disconnect Facebook at any time in your account settings.

Note: This processing only applies if you explicitly use the Facebook integration via Socials Hub. If you do not use this module, no Facebook-related personal data is processed or shared.

LinkedIn Integration

If you choose to use the option to automatically post news articles to your LinkedIn profile or page, the following applies:

- AS Support only receives and processes the data necessary to post news articles on your behalf via the LinkedIn connection.
- We do not share any other data with LinkedIn and will never post content without your permission.
- You can revoke this connection at any time via the platform or through your LinkedIn settings.

Instagram Integration

If you choose to use the option to automatically post news articles to your Instagram account, the following applies:

- AS Support only receives and processes the data necessary to post news articles on your behalf via the Instagram connection.
- We do not share any other data with Instagram and will never post content without your permission.
- You can revoke this connection at any time via the platform or through your Instagram settings.

Google Drive / Google Sheets Integration

If you choose to use the option to link your Google Drive and/or Google Sheets data to the AS Support newsletter module, the following applies:

AS Support only accesses and processes the data necessary to read relationship data from the Google files or spreadsheets selected by you or made available by you for this purpose.

Depending on the configuration of the integration, AS Support may process:

- selected Google Drive files and Google Sheets spreadsheets;
- spreadsheet content, including rows, columns, worksheet names, and cell values, only insofar as necessary to import, read, match, or synchronize relationship data with the newsletter module;
- file metadata, such as file name, spreadsheet ID, worksheet name, column headers, and last modified date;
- account and connection data necessary to maintain the integration, such as your Google account identifier, email address, and OAuth access or refresh tokens.

This data is used solely for the following purposes:

- establishing and maintaining the Google Drive / Google Sheets connection;
- reading and synchronizing relationship data with the newsletter module;
- supporting, troubleshooting, securing, and technically managing the integration;
- responding to user support requests relating to the integration.

Read-only access
The Google Drive / Google Sheets integration is configured and used on a read-only basis to the extent permitted by the selected functionality and granted permissions. AS Support does not create, edit, overwrite, or delete files, spreadsheets, worksheets, or data in your Google environment through this integration.

Limited use of Google user data
Google user data obtained through this integration is used exclusively to provide the functionality requested by the customer within the newsletter module. AS Support does not use this data for advertising, marketing profiling, resale, or any purpose unrelated to the operation, security, or support of the integration.

Storage and security
Where technically necessary, OAuth tokens or similar authorization credentials are stored in encrypted form and only for as long as required to maintain the active connection. Access to such credentials is restricted to authorized personnel and systems on a need-to-know basis.

Sharing of data
AS Support does not share Google user data obtained through this integration with third parties, except where this is strictly necessary for hosting, security, technical support, legal compliance, or the provision of the requested service.

Disconnecting the integration
You may revoke or disconnect the Google Drive / Google Sheets integration at any time through your account settings or through your Google account permissions settings. Once the integration is disconnected, AS Support will no longer access new data through that connection. Data already imported or processed within the newsletter module will only be retained insofar as necessary for the provision of the service, legal obligations, or legitimate recordkeeping requirements.

File Imports and External Integrations

If you use the option to provide personal data through file imports or through integrations with external services, the following applies.

AS Support only processes the data necessary to perform the functionality requested by you, such as importing, linking, synchronising, enriching, or managing relationship data within a module or other agreed service.

This may include:

- data contained in Excel, CSV, or similar files uploaded or provided by you;
- data obtained from external systems or data sources that you connect through an API or other technical integration;
- metadata such as file names, column headers, worksheet names, import mappings, modification dates, source identifiers, and logging data;
- technical authorization or connection data necessary to operate and secure the integration.

Such data is processed solely on your instructions and only insofar as necessary for the agreed services. AS Support does not use such data for advertising, profiling, resale, or any purpose unrelated to the delivery, security, or support of the requested functionality.

The customer remains responsible for the lawfulness, accuracy, and currency of the data provided through imports or external integrations and for being entitled to have such data processed by AS Support.

Why Do We Process Personal Data?

We process personal data only for the following purposes:

- Delivering websites, tools, and modules to customers.
- Processing data necessary for the services of our customers (e.g., mortgage or insurance applications).
- Securing our services and systems.
- Supporting our customers with requests from end users (such as access or deletion requests).
- Improving our services based on technical usage statistics.
- Importing, reading, linking, and synchronising relationship data from files provided by customers, such as Excel or CSV files.
- Importing, reading, linking, and synchronising relationship data from customer-activated external integrations, including API integrations and Google Drive / Google Sheets sources.

Controller and Processor

- **AS Support's customer is the data controller:** AS Support processes data on behalf of its customers (for example, data from end users entered via our tools).
- **AS Support is the processor:** We act only on instructions from our customers and take appropriate measures to secure personal data.

Legal Bases

We process personal data based on the following legal grounds:

- **Performance of a contract**: For example, to provide our services.
- **Legal obligations:** Such as fiscal retention requirements.
- **Legitimate interest:** Improving and securing our services.
- **Consent:** For specific processing, such as marketing.

For customer-activated imports and integrations with external platforms, such as Excel imports, API integrations, and Google Drive / Google Sheets, processing takes place insofar as necessary for the performance of the contract and, where applicable, on the basis of the authorization and instructions provided by the customer.

Data Retention and Deletion

We do not retain personal data longer than necessary for the purposes for which it was collected:

- **Contact details:** Up to 1 year after termination of the contract, unless legally required otherwise.
- **Financial data:** 7 years, in line with fiscal obligations.
- **Technical data:** Up to 6 months after processing.
- **Integration and authorization data:** OAuth tokens, API credentials, connection identifiers, and temporary technical synchronisation data relating to imports or external integrations are retained no longer than necessary to operate and secure the active import or integration functionality. Following revocation or termination of the integration, such data is deleted or rendered unusable, unless a limited retention period is required for security, audit, fraud prevention, or legal compliance purposes.

Immediately after termination of services, all personal data is securely and permanently deleted, unless otherwise agreed in writing.

Data Security

AS Support takes extensive technical and organizational measures to protect personal data against loss, misuse, and unauthorized access:

- Sensitive data is stored in encrypted databases.
- Authorization credentials for connected third-party services, including Google integrations where applicable, are stored encrypted and are accessible only to authorized systems and personnel strictly where necessary for service operation and support.
- For hosting, data center, and CMS development, AS Support only partners with ISO 27001/NEN 7510 certified companies.
- Customers log in with username, password, and optionally 2FA (two-factor authentication).
- Access to personal data is strictly limited to authorized staff and certified partners, only as necessary to provide our services.
- Authorization data for connected external services, including Google integrations and API connections, is stored in encrypted form and is accessible only to authorized systems and personnel insofar as necessary for the operation, security, and support of the relevant integration.

Rights of Data Subjects

End users have the following rights under the GDPR:

- **Access: The right to view their data.**
- **Rectification:** The right to correct inaccurate or incomplete data.
- **Erasure:** The right to have personal data deleted (“right to be forgotten”).
- **Restriction:** The right to restrict processing.
- **Portability:** The right to receive their data in a structured format.
- **Objection:** The right to object to processing based on legitimate interest.

Exercising Rights

Data subjects can exercise their rights by contacting us using the contact details in this policy. We respond to requests within 30 days. In exceptional cases, this period may be extended; we will inform the data subject in a timely manner.

Sub-Processors and Data Transfers

AS Support B.V. uses carefully selected certified partners (sub-processors) for parts of its services, such as hosting, data center services, and CMS management and development. For these sub-processors—including Rootnet B.V., BIT B.V., and LinkU B.V.—data processing agreements have been concluded, requiring them to protect personal data adequately and act in accordance with the GDPR.

For sending emails, AS Support B.V. uses SendGrid, based in the United States. Personal data such as email addresses and message content are only processed temporarily for email delivery. No data is stored at SendGrid after delivery; data is automatically deleted after sending, in accordance with SendGrid's policy. Transfers to the United States always take place with appropriate safeguards, such as the use of standard contractual clauses under the GDPR.

Where a customer uses an integration with Google Drive, Google Sheets, or another external service, data is exchanged with that external service provider chosen by the customer. Such processing takes place solely on the basis of the customer's activated integration and within the scope of the agreed functionality.

Data is otherwise only stored and processed within the European Economic Area (EEA). If processing outside the EEA is necessary, AS Support B.V. always ensures appropriate safeguards, such as using standard contractual clauses or working with parties in countries with an adequacy decision.

An up-to-date list of sub-processors is available upon request.

Data Breach Procedure

1. **Detection of a data breach:** Once a data breach is identified, AS Support records the incident in an internal log, including:
    - Date and time of discovery.
    - Data involved (if known).
    - Cause and impact of the breach.
    - In addition to data breaches, AS Support also informs customers of other serious security incidents that may affect the availability, integrity, or confidentiality of personal data.
2. **Notification to customers**
    - Within 48 hours of discovery, AS Support informs the customer of:
        - The nature of the data breach.
        - Which data may be affected.
        - Measures taken or recommended.
    - The notification includes sufficient detail for the customer (data controller) to comply with their own notification obligations.
3. **Measures**
    - AS Support immediately takes measures to stop the data breach and limit the impact. This may include:
        - Isolating affected systems.
        - Resetting access codes.
        - Adjusting security settings.
4. **Follow-up and reporting**
    - A full incident report is provided to the customer within 7 working days.
    - The report includes:
        - A summary of the incident.
        - Solutions implemented.
        - Any recommendations for future use.

Governing Language

This Privacy Policy is a translation of the original Dutch version. In case of discrepancies, the Dutch version shall prevail and is the legally binding document.

Contact Details

For questions about this privacy policy or to report incidents, please contact:

- AS Support B.V.
- Address: Frankenstraat 77, 6582 CW Heumen
- E-mail: servicedesk@assupport.nl
- Phone: +31(0)24-388 6998