SECURITY PROTOCOL SHEET — Route & Relax

Version 1.0 — 2026

Organization: Route & Relax (Eenmanszaak)
Owner: Dominika Paulina Janzowska
Location: Rosmalen ('s-Hertogenbosch), The Netherlands

This Security Protocol Sheet describes the technical and organizational measures used by Route & Relax to protect personal data and handle customer information with care in line with the AVG/GDPR.

1. Purpose of this document

The purpose of this protocol is to describe how Route & Relax protects personal data during business operations.

This includes:
- confidentiality: data is only accessible to authorized persons
- integrity: data remains accurate and is protected against unauthorized changes
- availability: data remains accessible where needed for service delivery and administration

2. Scope

This protocol applies to personal data processed during:
- contact requests
- custom edit requests
- full custom trip requests
- delivery of premade trips
- customer communication
- payment administration
- invoicing and bookkeeping
- storage, backup, and deletion procedures

It applies to the devices, systems, and business tools used by Route & Relax.

3. Roles and responsibilities

Data Controller:
Route & Relax

Owner: Dominika Paulina Janzowska

Access to personal data:
- only the business owner has direct access to customer data
- there are no employees or shared internal accounts at this time
- external providers may process limited data where needed to support the business

Examples of service providers may include:
- email provider
- website hosting provider
- payment provider (such as Mollie)
- secure storage, form, or website tools where applicable

The owner is responsible for data handling, security, and incident response.

4. Data categories covered

Route & Relax processes only the data needed to provide its products and services.

This may include:

Personal and contact data
- name
- email address

Travel-related data
- selected trip
- departure location
- destination or preferred region
- trip length
- travel group type
- travel preferences
- notes voluntarily provided by the customer

Administrative data
- invoice information
- payment reference or confirmation
- order-related communication

Sensitive personal data is not intentionally collected unless the customer voluntarily includes it.

Premade trips generally require less personal data than custom services.

5. Technical security measures

5.1 Device security
Devices used for business activities are protected through:
- strong passwords
- automatic screen lock after inactivity
- operating system security features
- regular updates
- antivirus and firewall protection where applicable

5.2 Data storage
- customer information is stored only where necessary for business use
- access is limited to the business owner
- unnecessary duplication of files is avoided
- backups are made where needed and kept securely

5.3 Email security
- email access is password protected
- customer communication is handled through the business email account
- personal data is not intentionally shared through insecure channels

5.4 Software and workflow tools
Route & Relax may use a combination of locally managed tools and trusted external business tools for:
- trip preparation
- PDF generation
- website operation
- payment handling
- communication and administration

Only the minimum necessary data is processed through these tools.

5.5 Website and payments
- the website should use HTTPS/SSL encryption
- payments are handled by a secure external payment provider, such as Mollie
- Route & Relax does not store full payment card or banking credentials itself

6. Organizational security measures

6.1 Access control
- only the owner accesses customer data directly
- no shared staff access
- no unnecessary account sharing

6.2 Data minimisation
- only data needed for the relevant product or service is collected
- premade trips require less data than custom requests
- unnecessary personal details are avoided

6.3 Device and workspace care
- devices are locked when unattended
- personal data is not printed unless genuinely necessary
- removable storage is avoided unless protected

6.4 Incident response
If a data incident is suspected, Route & Relax will:
- identify the affected system or file
- assess whether personal data may have been exposed
- reduce further risk where possible
- document the incident
- notify affected individuals where required
- report to the Autoriteit Persoonsgegevens within the required timeframe where legally necessary

7. Data retention and deletion

Retention periods may include:
- customer request and service data: up to 12 months where useful for support, updates, or follow-up
- bookkeeping and invoice data: retained as legally required
- payment records: retained only as needed for administration and compliance

Deletion measures may include:
- removal of unnecessary files
- deletion of expired customer records where legally possible
- cleanup of emails and stored documents when no longer needed

Customers may request deletion of personal data where legally possible.

8. International transfers

Route & Relax aims to use privacy-conscious tools and limit unnecessary international data transfers.

If a provider processes data outside the European Economic Area, appropriate safeguards should be in place where legally required.

9. Monitoring and review

This protocol is reviewed periodically and updated when:
- business processes change
- new service providers are introduced
- new technical systems are used
- legal or security requirements change

10. Contact information

For questions about security or privacy:

Route & Relax
Owner: Dominika Paulina Janzowska
Rosmalen ('s-Hertogenbosch), The Netherlands
Email: routenrelax@routenrelax.com