Data Processing Agreement

version 1.2 March 2022

Contents

1. Introduction
2. Basis
3. Parties
4. Validity of this document
5. Data
6. Sub-processors
7. Hosting and storage
8. Security
9. Data breach
10. responsibilities

1. Introduction

By using RogerRoger you are very likely to process sensitive personal data of customers, partners, suppliers and/or employees. Based on the GDPR legislation, you are responsible for this personal data and RogerRoger is a partner for analyzing it. By this agreement, you and RogerRoger agree to the terms of this partnership.

You give RogerRoger explicit permission in this agreement to process data on your behalf and you accept all responsibility and possible risks by working with RogerRoger's software. The basis of this agreement is the Dutch implementation of the GDPR, also known as AVG.

2. Basis

With this agreement you, as a customer or user of RogerRoger, are designated as responsible for all personal data. As a processor, RogerRoger helps you to analyze this data with its software.

3. Parties

The different parties to this agreement are us as: RogerRoger, Acsend BV or we. And you as: user, you, or customer.

4. Validity of this document

This agreement is effective when a new account is registered or when this agreement is accepted from your existing account. This agreement is valid until the account is completely deleted. It is not possible to terminate this agreement prematurely other than by deleting the RogerRoger account.

5. Data

As a RogerRoger user, you are responsible for all data that you process with RogerRoger. With the aim of gaining insights into communication between customers and employees.

6. List of sub-processors

To ensure that RogerRoger works optimally, we use sub-processors to perform certain tasks. We carefully select our sub-processors for continuity and reliability:

- *Nylas*: RogerRoger uses Nylas to read email accounts and emails. Nylas complies with SOC 2 type II and ISO:27001 standards. Data is stored and encrypted within the EU.

- *MailChimp*: With MailChimp we send emails for account registration and activation, password resets, updates and activities in RogerRoger. MailChimp is ISO:27001 certified and SOC 2 compliant.

- *Amazon*: Data is stored at Amazon AWS in Germany. Amazon's services are ISO:27001, ISO:27017 and ISO:27018 certified and SOC 2 compliant.

- *Intercom*: With Intercom we can provide you with a knowledge base and an option to chat with us directly.

- *Stripe*: RogerRoger uses Stripe to handle payments and subscriptions for the platform. These payments are handled by Stripe Payments Europe Limited based in Ireland. Stripe is a validated service partner of Visa and is a PCI Service Provider Level 1.

RogerRoger has agreements with the above sub-processors. These agreements are reviewed at least every year. By using RogerRoger you agree that RogerRoger uses

sub-processors.

7. Hosting and Storage

Data is stored within the EU on servers of TransIP, Amazon AWS and Platform.sh. These are located in the EU (Netherlands, Germany, France and Ireland).

8. Security

We believe it is important to handle your data and that of your customers with integrity. That is why we take various measures to ensure the security of your data:

- *Data center security*: RogerRoger uses Amazon servers at remote locations.

- *Secure connections*: We use SSL. All traffic to and from the RogerRoger API is secured with HTTPS. Traffic over HTTP is routed over HTTPS.

- *Firewall*: All servers are equipped with a firewall through which unwanted activities are detected and averted.

- *Separation of application and data*: RogerRoger is constructed in such a way that the application and data are technically and physically separated from each other.

- *Security Audits:* We periodically subject our software to penetration tests. We have this done by a specialized and certified external party.

9. Data breach

Despite the measures that we and our sub-processors take to meet all quality requirements, there is no 100% security guarantee for digital environments. In the event of a data breach, which affects your data, we will inform you within 5 days if possible. We will then tell you what the cause of the leak was, what the risks are and how we are going to solve this. Based on this information, other stakeholders (customers, suppliers, authorities) can be informed.

10. User Responsibilities

As a processor of personal data, you are responsible for the data you process with RogerRoger. As a processor, you are also responsible for obtaining permission to process such data. As a processor, you are also responsible for the correct security of the data. RogerRoger is not responsible for damages or claims based on the (illegal) data processed by the users.

Our contact details

RogerRoger

Lage Doelen 2

7772 BL Hardenberg (NL)

hello@rogerroger.io

+31 (0) 85 - 06 57 320