



# DATA PROCESSING AGREEMENT

**SURF AGENCY**  
*Surf the AI wave*

Last updated: November 17th 2025

Between:

**1. Surf Agency V.O.F.**

Registered at Burgemeester Oudlaan 50, 3062 PA Rotterdam, the Netherlands, registered with the Dutch Chamber of Commerce under number 97239402, hereinafter referred to as the “**Processor**”;  
and

**2. The Client,**

hereinafter referred to as the “**Controller**”.

Hereinafter jointly referred to as the “**Parties.**”

## **1. Background and Purpose**

The Processor provides services in the field of automation using artificial intelligence (AI), including the analysis and processing of customer data and the optimisation of business processes of the Controller.

In this context, the Processor processes personal data on behalf of the Controller. The Parties therefore enter into this Data Processing Agreement in accordance with Article 28 of the GDPR.

## **2. Purpose and Scope of Processing**

Processing of personal data is carried out solely for the purpose of performing the services provided by the Processor, including:

- Analysis of customer data belonging to the Controller;
- Automation of business processes using AI;
- Optimisation and integration of the Controller's ICT systems.

The Processor shall not process personal data for its own purposes.

## **3. Categories of Personal Data and Data Subjects**

The personal data may include, but are not limited to:

- Name, email address, phone number, address;
- Publicly available information (e.g., social media profiles);
- Data from CRM systems and other customer databases.

The data relate to:

- Employees of the Controller;
- Customers, end users, and prospects of the Controller;
- Partners or other relevant natural persons.

No special categories of personal data are processed.

## **4. Duration of Processing**

This Agreement enters into force upon acceptance by the Parties and remains effective for as long as the Processor processes personal data on behalf of the Controller.

Upon termination of the cooperation, the Processor shall, at the Controller's choice:

- Delete the personal data within 30 days; or
- Return the data in a commonly used format.

## **5. Obligations of the Processor**

The Processor guarantees that:

- Personal data are processed only on documented instructions from the Controller;
- Appropriate technical and organisational security measures are applied, including encryption, password protection, and two-factor authentication;
- The Processor provides reasonable assistance to the Controller in fulfilling GDPR obligations (such as access requests or data breach notifications).

## **6. Sub-processors**

The Processor may engage sub-processors, provided that:

- The Processor ensures that these sub-processors are bound by obligations equivalent to those set out in this Agreement;
- A list of sub-processors is provided upon request;
- The Controller is informed of significant changes in the sub-processor landscape.

The Controller hereby grants general authorisation for the use of sub-processors, including but not limited to:

- Google Cloud
- OpenAI
- n8n
- Lovable
- Supabase

## **7. International Data Transfers**

If personal data are transferred outside the European Economic Area, including to the United States, the Processor shall ensure that:

- The transfer complies with the GDPR;
- Appropriate safeguards are in place, such as Standard Contractual Clauses (SCCs) or other mechanisms approved by the European Commission.

## **8. Security Measures**

The Processor shall implement reasonable and appropriate technical and organisational measures to protect personal data against loss or unlawful processing, including:

- Secure connections (SSL/TLS);
- Password policies and access restrictions;
- Two-factor authentication;
- Secure storage and logging mechanisms.

These measures take into account the nature of the processing, risks to data subjects, and industry-standard security practices.

The Controller is responsible for ensuring the security of its own systems.

## **9. Audits and Inspections**

The Controller has the right to conduct an audit, once per calendar year and at its own expense, provided that:

- The Processor is notified in writing at least 30 days in advance;
- The audit is carried out in a manner that does not cause disproportionate disruption;
- Confidentiality is maintained at all times.

## **10. Personal Data Breach Notification**

The Processor shall notify the Controller without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach. The notification shall include:

- The nature of the incident;
- Categories and volume of affected data;
- Measures taken or proposed.

The Controller is responsible for notifying the supervisory authority and/or affected data subjects, where required.

## **11. ALiability**

The Processor's liability is limited to direct damages up to an amount equal to the fees paid by the Controller for the services during the twelve months preceding the incident, except in cases of intent or gross negligence.

The Processor shall not be liable for:

- Indirect or consequential damages;
- Loss of data due to incorrect instructions from the Controller;
- Fines imposed on the Controller by supervisory authorities.

## **12. Final Provisions**

- This Agreement forms an integral part of the Processor's general terms and conditions;
- In case of conflict between this Agreement and other agreements between the Parties concerning personal data processing, this Agreement shall prevail;
- This Agreement is governed by the laws of the Netherlands;
- Disputes shall be submitted to the competent court in Rotterdam.