



DATA PROCESSING AGREEMENT

In relation to the Account Verification for Businesses EU



THE UNDERSIGNED

This Data Processing Agreement (“DPA”) supplements the Terms of Service available at <https://www.surepay.eu/terms-of-service-corporates/>, as updated from time to time, between Customer and SurePay, or other agreement between Customer and SurePay governing Customer’s use of the Services. Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in the GDPR.

This DPA is entered into between you and the entity you represent (“Customer” or “Controller”) and SurePay BV, having its registered office in Utrecht, and for this agreement with place of business at Nicolaas Beetsstraat 222 3511 HG Utrecht, registered with the Chamber of Commerce, number 77251733 (hereinafter called “SurePay” or “Processor”).

CONSIDERING:

- The Parties entered into an Agreement for the distribution of the SurePay Account Verification Services for EU Corporates (the “Agreement”), which by reference includes the Terms of Service to be found at <https://www.surepay.eu/trust-center>;
- That SurePay is a Processor of personal data from Controller under this/these Agreement(s);
- That Parties agree that these Personal Data should be handled with care, integrity and confidentiality;
- That Customer is responsible for the processing of the Personal Data, and is therefore designated as the ‘Controller’ in accordance with the EU General Data Protection Regulation, with SurePay designated as the ‘Processor’ under these terms;
- That Controller instructs SurePay to process Personal Data as laid out in the Agreement and this DPA; and
- That Parties want to add and amend certain provisions in the Agreement in order to comply with the applicable laws regulations and guidelines, in particular the General Data Protection Regulation or Regulation (EU) 2016/679 (henceforth: “GDPR”);

AGREE AS FOLLOWS:

1. Definitions

In this Data Processing Agreement, the terms Data Subject, Record, Data Breach, Processor, Controller and Personal Data shall have the meaning assigned to them by the GDPR.

2. Data Protection

2.1. The following arrangements shall apply for processing of personal data as defined in the GDPR:

i. SurePay processes personal data on behalf of Controller or parts of the Controller Group within the scope of the Agreement. This agreement shall be regarded as a data processing contract as defined in article 28 of the GDPR; ii. SurePay shall process personal data in a proper and careful manner and in accordance with the GDPR and all other applicable laws and regulations; iii. Processing of personal data shall exclusively take place for the proper performance of the Agreement, and in accordance with the written instructions of Controller as laid down in the Agreement; iv. The terms of the Agreement apply in full to this Data Processing Agreement. Likewise, the provisions of all Appendices to this Data Processing Agreement form an integral part of this Data Processing Agreement. Insofar as there are any inconsistencies between the Agreement and this Data Processing Agreement, the Agreement shall prevail, unless this Data Processing Agreement explicitly states that it varies from the Agreement, indicating the specific element affected.



3. SurePay's Obligations

3.1. SurePay has no independent control over the Personal Data and shall process this Personal Data only by order of the Controller and in accordance with the latter's written instructions in the Agreement and the agreed purposes and means by which personal data is processed. SurePay may not process the relevant Personal Data for its own benefit, for the benefit of third parties or for other purposes, except where such permission has been granted by Controller.

3.2. SurePay is explicitly prohibited from processing the Personal Data or allowing the Personal Data to be processed in any way other than described in the Agreement or this Data Processing Agreement.

3.3. At the request of Controller, SurePay will provide all reasonably necessary assistance, for instance: provide all co-operation so that the data subjects receive: access to their personal data at their request or have personal data removed or corrected.

4. Duty to cooperate regarding Data Subject's Right of Access

4.1. SurePay shall fully cooperate with Data Subjects and Controller to allow Data Subjects, at their request, to (i) access their Personal Data, (ii) have Personal Data deleted or corrected, and/or (iii) obtain proof that Personal Data has been deleted or corrected if it is incorrect, or if the Principal disputes the Data Subject's claim, to record the fact that the Data Subject considers its Personal Data to be incorrect. SurePay shall for this purpose always redirect Data Subjects to Controller since SurePay is unable to make these modifications itself.

5. Sub-Processing

5.1. SurePay shall exclusively allow the Personal Data to be accessed by those employees, agents and/or third parties for whom access to the Personal Data is necessary for the proper performance of the Agreement.

5.2. SurePay shall ensure that the employees, agents and/or third parties it enlists shall comply with the obligations regarding protection and confidentiality determined in this Data Processing Agreement and in the Agreement and shall bear full responsibility for this compliance.

5.3. SurePay will, when enlisting a new sub-processor related to the processing Controller's data, inform Controller of said new sub-processor as far as possible in advance. If Controller wishes to object to SurePay's use of said sub-processor, Controller can raise a formal written objection. This objection may be paired with a potential temporary suspension of Service where Controller cannot accept said sub-processor, and said sub-processor is already live in production for the Service. Parties shall then jointly decide how to proceed with the use of sub-processors. Where after 30 Dutch business days, the Parties cannot reach a joint decision, Controller may terminate the Agreement without incurring any liability under the Agreement or under this Data Processing Agreement.

6. Personal Data Transfers

6.1. Any transfer of Personal Data to Processor or any Third Party in a Non-Adequate Country shall be governed by adequate protection mechanism, for instance: the terms of the EC Standard Contractual Clauses. SurePay shall ensure that all Sub-Processors in a Non-Adequate Country sign the EC Standard Contractual Clauses or have other adequate protection mechanisms in place to protect the Personal Data. Processor and Controller shall work together to apply for and obtain any permit, authorisation or consent that may be required under Data Protection Law in respect of the implementation of this Clause 6.1.

7. Technical and Organisational security measures for Personal Data

7.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, SurePay shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

7.2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised Disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.



7.3. SurePay works in accordance with ISO27001 and has an appropriate security policy in writing that has been implemented for the Processing of Personal Data and in any event describes the measures stated in this Clause 7.

8. Notifications of Disclosures and Personal Data Breaches

8.1. SurePay shall without undue delay and, where feasible, not later than 48 hours after having become aware of it, notify Controller in accordance with Clause 13 if:

- 8.1.1.** it receives an inquiry, a subpoena or a request for inspection or audit from a competent public authority relating to the Processing, except where Processor is otherwise prohibited by law from making such disclosure;
- 8.1.2.** it intends to Disclose Personal Data to any competent public authority, if permitted by law; or
- 8.1.3.** it detects or reasonably suspects that a Personal Data Breach has occurred.

Where a notification pursuant to this Clause is not made within 48 hours, it shall be accompanied by valid reasons for the delay.

8.2. A notification pursuant to Clause 8.1. shall include (i) the nature of the Personal Data breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, (ii) the date and time upon which the Personal Data Breach occurred, (iii) a description of the likely consequences of the Personal Data Breach, (iv) whether and, if so, which measures were taken to mitigate possible adverse effects of the Personal Data Breach and (v) any further information necessary for Controller to comply with Personal Data Breach notification requirements under Data Protection Law.

8.3. SurePay is not responsible for legitimate grounds of Data Processing under this Agreement. The purpose and grounds for Processing Personal Data under this Agreement are decided by the Controller. As such, SurePay is not responsible for any and all Personal Data Breaches resulting out of / or other non-compliance by Controller with GDPR legislation or other applicable privacy regulations. Controller takes full responsibility for said infringements of data protection regulations.

9. Notification of non-compliance and right to suspend or terminate

9.1. SurePay shall as soon as reasonably possible notify Controller if SurePay:

- 9.1.1.** cannot for any reason comply with its obligations under the Annex;
- 9.1.2.** becomes aware of any circumstance or change in Data Protection Law that is likely to have a substantial adverse effect on SurePay's ability to meet its obligations under the Annex or Agreement; or
- 9.1.3.** believes that an instruction by Controller related to the Processing infringes Data Protection Law.

9.2. Without prejudice to the termination clause(s) of the Agreement, SurePay may temporarily suspend the Processing in whole or in part if it, for any reason, is unable to meet its obligations under the Annex until such time that the non-compliance is remedied. This shall be governed by clauses in the Agreement.

10. Return and deletion of Personal Data

10.1. Where reasonably possible, all Personal Data shall be immediately returned to Controller, or destroyed by SurePay, upon termination of the Agreement except to the extent the Agreement or Data Protection Law provides otherwise. In that case, SurePay shall no longer Process the Personal Data, except to the extent required by the Agreement or Data Protection Law, or where it is not reasonably possible to destroy such data due to technical constraints. SurePay shall not retain Personal Data any longer than specified under the Agreement and in this Data Processing Agreement.

11. Inspection or audits by public authorities

11.1. In addition to the audit obligations laid down in the Agreement, either Party shall submit its relevant Processing systems, facilities and supporting documentation to an inspection or audit relating to the Processing by a competent public authority if this is necessary to comply with a legal obligation. In the event of any inspection or audit, each Party shall provide all reasonable assistance to the other Party in responding to that inspection or audit. If a competent public authority deems the Processing unlawful, the Parties shall take immediate action to ensure future compliance with Data Protection Law.



12. Term and Termination

12.1. This Data Processing Agreement shall be in effect jointly with the Agreement. Where the Agreement were to be terminated, this Data Processing Agreement shall be considered terminated as well.

12.2. Clause 12.1 shall not apply to those clauses which are reasonably understood to survive the termination of the Agreement, and are necessary for the final execution and applicability of Data Protection laws. Neither shall Clause 12.1 adversely affect any of the obligations and severable clauses contained in the Agreement.

12.3 This Data Processing Agreement shall commence where countersigned and received by SurePay in the designated format as set out in this Data Processing Agreement, and shall run as long as the Agreement remains in effect.

13. Notices

13.1. All notices, confirmations and other statements made by the Parties in connection with this Annex shall be in writing and shall be in accordance with the relevant clauses of the Agreement.

14. Prevalence of the Agreement

14.1. In the case of conflict between the provisions contained in this DPA and the clauses as provided per the Agreement and its appendices. This DPA shall take precedence over the body of the Agreement and its appendices to the extent that it is required by relevant Data Protection legislation.

15. Jurisdiction

15.1. The jurisdiction to which this DPA is subject shall be same jurisdiction as is mentioned in the Agreement. If no explicit jurisdiction is decided upon in the Agreement, the exclusive jurisdiction over this DPA shall be Dutch law (including non-contractual disputes and claims). The sole competent court shall in that case be the courts of Utrecht, the Netherlands.



THUS AGREED AND SIGNED IN DUPLICATE:

SurePay B.V.

Name: David-Jan Janse | CEO

Name: Ralf van den Berg | CFO

Customer

Name:

Title:

Date:

Name:

Title:

Date:

Please return countersigned to SurePay at: corporate-support@surepay.io for this document to enter into force.



SCHEDULE 1

A. Categories of Data Subjects

The Personal Data being Processed concerns - to the extent relevant for the performance of the Agreement - the following categories of Data Subjects

- Existing and prospective customers, creditors and debtors of Controller or their Employees;
- Data Subjects making requests, enquiries, or providing information.

B. Categories of Personal Data

The Personal Data being Processed concern - to the extent relevant for the performance of the Agreement - the following categories of Personal Data:

- **Personal Details and Contact Information:** Name; address; email; telephone details and other contact information.
- **Professional Details:** Title; company and department or other professional affiliation.
- **Operational Data:** Bank account number, User ID, usage data, access logs, activity logs, and electronic content produced by Data Subjects; IP address and other device identifiers.
- **Other Personal Data:** Such other Personal Data that the Data Subject may provide within the context of the Agreement, or that are relevant to SurePay's relationship with the Data Subject or that the Data Subject chooses to provide to SurePay, such as reviews, opinions and complaints about SurePay's products and services.

C. Purposes of the Processing

The Personal Data being Processed concern - to the extent relevant for the performance of the Agreement - the following purposes:

- **Communications:** Facilitating communication between the Parties and their personnel in the context of the execution of the Agreement.
- **Business Operations:** Providing products and services under the Agreement, including the operating and managing of the relevant IT and communications systems.
- **Compliance:** Complying with legal, tax and other requirements, such as recordkeeping and reporting obligations.