

Data Processing Agreement

Effective as of April 2020 Last updated March 2020

Between:

Catering Angel, 66 Middleton Close, Warwick, United Kingdom (hereinafter "the Customer" or "Data Controller")

And

SumUp Limited, Block 8, Harcourt Centre, Charlotte Way, Dublin 2, Ireland D02 K580, VAT: IE9813461A (hereinafter "SumUp" or "Data Processor") each a "party"; together "the parties", HAVE AGREED to the terms of this Data Processing Agreement (hereinafter the "DPA" or "Agreement") on Personal Data Protection regarding the processing of Personal Data when the Customer is acting as Data Controller and SumUp is acting as Data Processor, to fulfill the service obligations outlined in the Terms and Conditions of SumUp Accounting and Invoices in the Services Agreement (detailed below). As part of the fulfilment of those service obligations, SumUp will process certain Personal Data on behalf of the Data Controller, in accordance with the terms of this contract. Each party agrees and will ensure that the terms of this contract shall also be fully applicable to its Affiliates which may be involved in the processing operations of Personal Data for the project defined in the Terms and Conditions of SumUp Accounting and Invoices, in the Services Agreement. Specifically, SumUp will ensure that all Sub-Processors operate within the same terms as this Agreement when processing Customer's Personal Data. For the purposes of the personal data processing under this DPA, SumUp uses as a sub-processor, an entity, part of SumUp Group - Debitoor Ireland Ltd. Block 8 Harcourt Centre, Charlotte Way, Dublin 2, D02 K580 ("Debitoor").

Introduction and Definitions

Personal Data is defined as any information relating to a data subject by which it can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person or legal entity (where applicable).

All other definitions referred to herein, including the terms Data Controller and Data Processor, are as determined by the relevant Data Protection laws, including EU General Data Protection Regulation Regulation 2016/679 of 27 April 2016 (hereinafter "GDPR").

Sensitive Personal Data is not deemed to be processed under the Application Service offered by the Data Processor (SumUp Accounting and/or Invoices) and so is excluded from the terms of this Agreement.

By signing up to use the SumUp Accounting and/or Invoices program and accepting the Terms and Conditions, including the Privacy Policy and this DPA, the parties agree under all national data protection laws and under GDPR that this Agreement governs the relationship between the Data Controller and the Data Processor, determining the processing of personal data by SumUp of the Customer's data. This Agreement takes precedence unless it has been replaced by another signed DPA which communicates its precedence over this Agreement.

The purpose of SumUp's processing of Personal Data for the Customer is to ensure the Customer's full use of the Service and to allow this Agreement to be fulfilled. SumUp ensures that sufficient security of Personal Data is maintained at all times.

Both parties confirm their Authority to sign the Agreement by so doing.

Data Processor Responsibilities

The Data Processor must handle all personal data on behalf of the Data Controller and following their instructions. By entering into this Agreement, SumUp (and any sub-processors whom the Data Processor has legal agreement for services with) is instructed to process Personal Data of the Customer:

1. In accordance with all national and European laws
2. To fulfil its obligations under the Terms and conditions for SumUp Accounting and Invoices
3. as further instructed by the Data Controller
4. as described in this Agreement

As part of providing the Application, the Data Processor is required to always provide the Customer with adequate solutions to accompany continued development of their business by using the service. The Data Processor tracks how the Customer use the Application in order to make the best suggestions, to provide relevant services at all times and to engage in sending the most accurate communications to aim towards continued ease of use and satisfaction. As far as the processing of personal data from the Application form part of this, they are processed only in accordance with this DPA and applicable law and are shared only as required to provide a better experience for the Customer.

Taking into account the available technology and the cost of implementation, as well as the scope, context and purpose of the Processing, the Data Processor is required to take all reasonable measures, including technical and organizational measures, to ensure a sufficient level of security in relation to the risk and the category of Personal Data to be protected. The Data Processor shall assist the Data Controller with appropriate technical and organizational measures as required and taking into account the nature of the treatment and the category of information available to the Data Processor to ensure compliance with the Data Controller's obligations under applicable Data Protection laws.

The Data Processor shall notify the Data Controller without undue delay if the Data Processor becomes aware of a security breach.

In addition, the Data Processor shall, as far as possible and legally, inform the Data Controller if a request for information on data held is requested (Data Access Request) by any bodies to whom they should provide it. The Data Processor will respond to such requests once authorized by the Data Controller to do so. The Data Processor will also not disclose information about this Agreement unless the Data Processor is required by law to do so, such as by court order.

If the Data Controller requires information or assistance regarding the security of data, documentation or information about how the Data Processor processes Personal Data generally, they can request this information of the Processor.

The data processor, its employees and any Affiliates, shall ensure confidentiality in relation to Personal Data processed under the Agreement. This provision continues to apply after termination of the Agreement, regardless of the cause of termination.

Data Controller Responsibilities

The Data Controller confirms, by signing/accepting this agreement, that it will, when using the Application, be able to freely process its data once in line with all Data Protection legal requirements including GDPR. They are giving explicit consent to the processing of their Personal Data at all times when using the Service.

The Data Controller can revoke the acceptance of this DPA at any stage, but by doing the Data Processor will no longer be able to provide the Service.

The Customer has a legal basis for processing the Personal Data with the Data Processor (including any sub-processors) with the use of SumUp's services.

The Data Controller is responsible at all times for the accuracy, integrity, content and reliability of the Personal Data Processed by the Data Processor. They have fulfilled all mandatory requirements in relation to notification to, or obtaining permission from the relevant public authorities regarding the Processing of Personal Data. They have further fulfilled their disclosure obligations to the relevant authorities regarding the processing of Personal Data in accordance with all applicable data protection legislation.

The Data Controller must have an accurate list of the categories of Personal Data it processes, particularly if such processing differs from the categories listed by the Data Processor in Appendix A.

Agreement to Data Transfer and the Use of Subcontractors

In order to provide the service to the Data Controller, the Data Processor may use sub-processor (or "subcontractors"). These subcontractors can be third party suppliers both within and outside the EU / EEA. The data processor ensures that all subcontractors satisfy the obligations and requirements within this agreement, specifically that their level of data protection meets the standard required under relevant Data Protection laws. If a jurisdiction falls outside of EU / EEA and is not on the European Commission approved listing of satisfactory data protection levels under GDPR, then specific agreement is entered into between SumUp and such subcontractor to assure they will maintain all Personal Data in line with the requirements under current EU Data Protection laws.

This Agreement constitutes the Data Controllers prior specific and explicit consent to the Data Processor's Use of subcontractor Data Processors which may at times be based outside the EU / EEA or territories approved by the European Commission.

The Data Controller can revoke this consent at any stage, but by doing so terminates the Agreement in place and the Data Processor will no longer be able to provide Service.

If a Subcontractor is established or stores Personal Data outside of the EU / EEA or European Commission approved territories, the Data Processor has the responsibility to ensure a satisfactory

basis for transferring Personal Data to a third country on behalf of the Data Controller, including the use of the EU Commission Standard Contracts or specific measures which have been pre-approved with the EU Commission.

The Data Controller must be informed before the Data Processor replaces its Subcontractors. The Data Controller can then object to a new Sub-Processor who processes their Personal Data on behalf of the Data Processor, but only if the Sub-Processor do not process data in accordance with relevant data protection legislation. The Data Processor can demonstrate compliance by providing the Data Controller with access to the data protection assessment conducted by the Data Processor.

If the Data Controller still objects to the use of the Subcontractor, they may terminate their subscription to the Service, without the usual notice period required, then ensuring that their Personal Data is not processed by the non-preferred subcontractor.

Duration of the Agreement

The agreement remains valid as long as the Data Processor processes Personal Data with the Data Controller's use of the Service Application and unless it is replaced by another signed DPA which communicates its precedence over this Agreement.

Termination of the Agreement

Should the data controller decide to stop using the service, whether the service is via subscription or not, the data controller can also delete all their account data. Upon the execution of the data deletion procedure initiated by the data controller, the Data Processor deletes all Personal Data, except that which they are required to retain under any applicable legal requirements, and in such case will be held in accordance with the technical and organizational safeguards within SumUp.

The Data Controller has full capability to retrieve all of their Personal Data within the Service Application. If the Data Controller requests data retrieval assistance, the associated costs shall be determined in agreement between the Parties and shall be based on the complexity of the requested process and the time to fulfil it in the chosen format.

Changes to the Agreement

Changes to the Agreement might be made by the Data Processor in a separate Annex to the Agreement or another visible way for the Data Controller and communicated to the Data Controller. If any of the provisions of the Agreement are deemed invalid, this does not affect the remaining provisions. The parties shall replace invalid provisions with a legal provision that reflects the purpose of the invalid provision.

Audits

The Data Controller is entitled to initiate a review of the Data Processor's obligations under the Agreement once a year. If the Data Processor is required to do so under applicable legislation, audits may be repeated once a year. The Parties decide together if a third party should conduct the audit. However, the Data Controller may allow the Data Processor to have the security review by a neutral third party of the Data Processor's choice, if it is a processing environment where multiple data controller data is processed.

If the proposed scope of the audit follows an ISAE, ISO or similar certification report conducted by a qualified third-party auditor within the previous twelve months and the Data Processor confirms that there have been no material changes in the measures under review, this will satisfy any requests received within such time frame. Audits may not unreasonably interfere with the Data Processor's business as usual activities. The Data Controller is responsible for all costs associated with their request for audit review.

Responsibilities and Jurisdictions

Liability for actions arising from breach of the provisions of this Agreement is governed by liability and compensation provisions in the Terms and Conditions of SumUp Accounting and Invoices. This also applies to any violation by the Data Processor Sub-Processors. This Agreement is governed by and construed in accordance with Irish law and the Irish courts will have Irish exclusive jurisdiction to determine any dispute concerning the same.

Appendix A - Categories of Personal Information and Usual Processing Categories

A. Categories of Personal Information (list is non-exhaustive)

- Name
- Address

- Telephone number(s)
- Email address(es)
- Address(es)
- Any account numbers and/or bank details

B. Usual Processing Categories (list is non-exhaustive)

- The Data Controller's Employees
- The Data Controller's Contacts (telephone/email/addresses/etc) The Data Controller's Customers
- The Data Controller's Banking information
- Their Customer's Employees
- Their Customer's Contacts (telephone/email/addresses/etc) Their Customer's Customers
- Their Customer's Customers Banking information