Privacy Policy

- Updated on March 18th 2018 to include GDPR requirements
- Updated on November 16th 2020 to change the SumUp entity acting as a data controller
- Updated on November 10th 2021 to include information about cash advance products
- Updated on April 14th 2022 to include information about data sharing
- New version updated on January 16th 2023

Table of content

This Privacy Policy describes how SumUp and its affiliates (collectively, "SumUp," "we," "us", "SumUp Group") collects, uses, discloses, retains or otherwise processes your information when you use our products and services under the SumUp brand, including our software, hardware, mobile applications, access or sign up at our mobile applications, ("App"), and websites ("Website"), when you speak to our staff, or when you otherwise interact with us (collectively, the "Services"). This Privacy Policy also applies to information we collect if you have not signed up for our Services, but if you are making and/or receiving payment transactions through our Services.

This Privacy Policy does not apply for services provided directly to end-users, physical persons, for their personal and not business use ("Personal Services"), including usage of the mobile app SumUp Pay and using gift cards issued by SumUp's Merchants (if available in your country). Please read our specific Privacy Policy for Personal Use.

Please read this Privacy Policy carefully. If you have any privacy related questions, please contact us at dpo@sumup.com.

Who is the data controller?

The SumUp Group is made up of different companies. We will let you know which SumUp entity you have a relationship with when you first apply for, or use, a SumUp Service. The SumUp company providing the relevant product or Service to you will be responsible for processing your personal data for that product or Service. This SumUp company is known as the 'controller' of your personal data.

For our business in Europe, typically one of the following entities is the data controller:

- **SumUp Payments Limited**, authorised by the Financial Conduct Authority under the Electronic Money Regulations 2011, a company with limited liability incorporated in England and Wales with its registered number 07836562 and with its registered office at 16-20 Shorts Gardens, London WC2H 9US, UK. SumUp Payments Limited is registered as a data controller with the Information Commissioner's Office under registration number ZA265663.
- **SumUp Limited**, company with limited liability incorporated in Ireland with its registered number 505893, and with its registered office Block 8, Harcourt Centre, Charlotte Way, Dublin 2, Ireland D02 A9N9. SumUp Limited is an authorised Electronic Money Institution (license no. C195030, issued on 27 October 2020) regulated by the Central Bank of Ireland.
- **SumUp EU Payments, UAB,** electronic money institution licensed by the Bank of Lithuania (license No. 56, issued on August 27, 2019), with registered address Ukmergės g. 126, 08100 Vilnius, Lithuania and company number 305074395.

This Privacy Policy concerns the processing of personal data for which we are the data controller – in other words, where we decide the purposes (why the personal data is collected) and means (which personal data is collected, for how long it is stored, etc.) of the processing. When we act as a data processor on behalf of another controller and/or our Merchants, we collect, use, and disclose certain personal information only under the controller's instruction, and our processing of your personal information is subject to their instructions and privacy

policies. Links to third-party websites are subject to the third-parties' privacy policies and terms of use, not ours, unless clearly stated otherwise.

In relation to whom are we a data controller?

Depending on the context, "**you**" means:

- When you directly use an End User Service (such as when you sign up for SumUp Pay, or use our Services in your personal capacity), for your personal use, we refer to you as an "**End User**." Please read our specific Privacy Policy for Personal Use.
- When you directly use a Merchant Service (typically using SumUp Services with your created SumUp Account/Profile) for business purposes and if you are a natural person – sole trader or an individual, we refer to you as a **"Merchant".**
- When you are acting on behalf of an existing or potential Merchant (e.g. you are a beneficial owner, shareholder, officer, director, account representative or other legal representative), we refer to you as a **"Representative of a Merchant".**
- When you do business with, or otherwise transact with a Merchant (typically a merchant having a SumUp Account/Profile) but you are not directly doing business with SumUp, we refer to you as an **"End Customer**" or "**Merchant's Customer**".

For some of the Services we provide to End Customers we act as a Merchant's service provider and we act as a data processor on behalf of the Merchant - when you are an End Customer of Merchants who process your data for their own purposes and own legal grounds (when Merchants are using our Invoicing and Accounting Services, Online Store, Gift Cards, POS solution and/or customer directory as part of a Service we offer).

We are the data controller for the processing of personal data that takes place when an End Customer chooses to pay for the services and/or products provided by any of our Merchants who use SumUp for processing payments in their physical store or online store, as applicable. Such payment may be done by different

means including by card or smartphone, tablet or other compatible mobile device enabling the End Customer to take contactless smartphone/device transactions, via QR code, through a payment link provided by e-mail, text message or similar communication tool, online by card in Merchant's online store, through the use of third payment providers.

We are also the data controller when End Customers want to enable Automatic Receipts for the services and/or products provided by any of our Merchants who use SumUp and/or earn loyalty points with our Merchants.

This Privacy Policy covers only the data processing activities for which we act as a data controller for End Customer's Data.

- When you visit our Website without being logged into a SumUp Account/Profile or otherwise communicate with SumUp, we refer to you as a "**Visitor**" (e.g. you send SumUp a message asking for more information because you are considering being a user of our products).
- When you enter into a contractual relationship with us (if you are a natural person – sole trader or an individual, or legal representative of a company) and provide us with a specific service or product, we refer to you as a **"Vendor".**
- When you want to enter into a business partnership with SumUp (if you are a natural person – sole trader or an individual, or legal representative of a company) and work with us by referring potential merchants and promoting our Services and brand, we refer to you as a "**SumUp Partner".**

If we provide you with a specific Privacy Policy before processing of your data, different than the present one, please read it carefully. It may be the case that we have decided to provide you with a Service/role specific Privacy Policy for your convenience.

What information do we process about you, for what purposes and how is it lawful for us to do it?

Merchants and representative of our merchants (as applicable)

Please note that if you do not provide us with the requested information as part of your SumUp **Account/Profile Registration**, including your **identification data** or other data as requested by us as part of **know your customer related information**, we may not be able to provide you with our Services.

You will be promptly informed for the required data provision throughout your Account/Profile registration process or during the lifetime of the relationship (as applicable) with us.

Please note that we need these data in order to enter/continue our contractual relationship with you and comply with our legal obligations.

End Customer

Partners and vendors

Visitors

Children’s personal information

Our Services are not directed at children under the age of 18. If we learn that any information we collect has been provided by a child under the age of 18, we will promptly delete that information.

Your rights and privacy choices

a. Choices related to communication and marketing

If you have received marketing from us, you may at any time object to the marketing. The easiest way to do so is to opt out by following the instructions in the marketing material that you have received. Also, you can opt-out by changing your notification settings in your SumUp Account/Profile or by contacting us at dpo@sumup.com with clear instruction that you don't want to receive marketing communication from us anymore.

Please note that we may continue sending you communication that is required or necessary for the provision of our Services, including providing such notifications that include important information and other communication that you request from us. You may not opt out of receiving these communications.

b. Your data protection related rights

SumUp is happy to assist you in exercising your rights under data protection law. You have the right to:

- **Be informed** – you have the right to be informed about how we process personal data about you. We do this in this Privacy Policy. Nevertheless, you may always contact us if you have any further questions.
- **Access** to your personal information that we process.
- **Rectification** – you can ask SumUp to update, complete or correct any inaccurate personal information. This right always applies.

- **Erasure** – have your personal data deleted under certain circumstances, if your data is no longer necessary for the purposes for which it was collected, and we have no legal ground for processing the data. Just to let you know, we may not be able to agree to your request. As a regulated payment services provider, we must keep certain customer personal data even when you ask us to delete it. We may not be able to delete your entire file because these regulatory responsibilities take priority. We will always let you know if we can't delete your personal data.
- **Data portability**. This only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organisation to another or give it to you. The right only applies if we are processing information based on your consent or under, or in talks about entering into a contract and the processing is carried out by automated means.
- **Restrict the processing** of your information under certain conditions.
- **Object to the processing** of your personal information (if we are using it for our legitimate interests). If our legal basis for using your personal data is 'legitimate interests' and you disagree with us using it, you can object. However, if there is an overriding reason why we need to process your personal data, we will not accept your request.
- Withdraw your consent to SumUp using your personal information (please note, if you take back your consent, this will not affect our use of your personal information before you notified us that you no longer consent).
- Carry out a human review of an automated decision we make about you. If we make an automated decision about you that significantly affects you, you can ask us to carry out a manual review of this decision.

You can exercise your rights by sending an email to dpo@sumup.com.

If you are authorised to set the SumUp Account up, or give us instructions about the account (for example, you are Merchant's Representative or the Merchant, if sole trader or freelancer), you can send us an email at dpo@sumup.com or contact us via the dashboard when you are logged into your SumUp Acccount/profile (if you have one).

If you are an employee of the Merchant is responsible for helping you with your request.

For security reasons, we can't deal with your request if we are not sure of your identity, so we may ask you for additional data to verify you, if this is proportionate to the request. If a third-party exercises one of these rights on your behalf, we may need to ask for proof that a third party has been validly authorized to act on your behalf.

When you exercise one of these rights, we have one month to respond to you. SumUp will usually not charge you a fee when you exercise your rights. However, we are allowed by law to charge a reasonable fee or refuse to act on your request if it is manifestly unfounded or excessive.

If you are not satisfied with how we process your data, you have the right to lodge a complaint with us and/or with the relevant data protection authority. SumUp will cooperate fully with any such investigation and endeavor to satisfy all queries as fully as possible. The relevant authority for each country can be found on the European Commission website: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080.

Please note that we only are directly responsible to you in cases where we are the controller of your personal information. Where we are acting as a data processor, you should contact the third party who is the data controller of your personal information.

Automated decision making and profiling

Automated decision making is the process of making a decision by automated means without any human involvement. Profiling means analysis of an individual's personality, behaviour, interest and habits to make predictions or decisions about them. There are such solely automated decisions, that could have a legal or similarly significant effect on you as an individual. We may in some cases use

automated decision-making for decisions, if authorized under applicable law or where necessary for the entry into or performance of a contract.

You can always ask for a manual decision-making process instead, express your opinion or contest decision making based solely on automated processing, including profiling, if such a decision would produce legal effects or otherwise similarly significantly affect you.

Please contact us at dpo@sumup.com if you require more information on automated-decision making.

Personal data collected from third parties

We may collect information from sanctions lists held by international organisations registers held by credit-rating agencies and other commercial information providers providing information on e.g. beneficial owners and politically exposed persons.

We process personal data obtained from selected third parties such as credit bureaus, fraud detection agencies, other financial institutions and other information providers, and from publicly available sources (such as population registers and registers held by tax authorities, company registration offices, enforcement authorities etc). In connection with payments we collect information from e.g. banks, payment service providers and others.

Data sharing with third parties

Your data will only be processed and shared in connection with the Services and in accordance with this Privacy Policy and applicable data protection legislation. We may share your data as follows:

- **SumUp Group.** We may share personal information with members of the SumUp Group for the purposes set out in this Privacy Policy. This data may be transferred to allow us to provide a full service to you, where other companies within our group perform components of the full-service offering. These other services include customer support, anti-money laundering, settlements, internal audit and others.
- **Third party providers**. To provide our Services we disclose personal data about you which is necessary to identify you and perform an assignment or agreement with companies that we cooperate with in order to perform our Services. These services include, but are not limited to, secure identification solutions, fraud prevention and credit bureaus in the relevant country and between parties in the financial system such as banks.

Cifas. If you are registered in the UK, the personal information we have collected from you will be shared with fraud prevention agencies who will use it to prevent fraud and money-laundering and to verify your identity. If fraud is detected, you could be refused certain services, finance, and employment. Further details of how your information will be used by us, these fraud prevention agencies, and your data protection rights, can be found here https://www.cifas.org.uk/fpn.

- For UK license activity only: If you have registered and signed up for SumUp Account/Profile with us, we may check your credit history with accredited credit reporting agencies, to help us develop and offer selected credit products in accordance with your needs, including pre-filtering of credit products. These checks will have no impact on your credit history.

For the above purpose we use the following credit reporting agencies:

Equifax (Equifax.co.uk) - https://www.equifax.co.uk/crain/

Experian (Experian.co.uk) - https://www.experian.co.uk/legal/crain/

- **Third parties independent data controllers.** Some of the third parties that we share personal data with are independent data controllers. This means that we are not the ones that dictate how the data that we provide shall be processed. Examples are authorities, acquirers and other financial institutions. When your data is shared with independent data controllers their data policies and personal data processing principles apply.We may disclose your personal information to professional advisors, such as lawyers, bankers, auditors and insurers, where necessary in the course of the professional services that they render to us.
- **Acquiring partners and parties in the payment processing.** Where we provide payment services to you, or your company, we may share some of your, or your customers', personal data with our third party acquiring partners. This is necessary to provide you with the payment services you have requested. We can share information about you with financial institutions, processors, payment card associations and other entities that are part of the payment processing and collections process.
- **Third parties that are data processors.** Some of the third parties that we share personal data with are data processors. A data processor is such a party that processes personal data on our instructions and on our behalf. We collaborate with selected suppliers, which include processing of personal data on behalf of us. Examples include suppliers of IT development, maintenance, hosting and support but also suppliers supporting us with marketing. When we share your personal data with data processors we only share them for purposes compatible with the purposes for which we have collected the data (such as performance of a contract). Our contracts dictate that these service providers only use your information in connection with the services they perform for us and not for their own or any others' benefit.
- **Partners**. We may share minimal personal information (such as your business name) with potential partners who may be able to provide a complementary or related service for your business.
- We may disclose information collected about you with third parties in connection with any merger, sale of company shares or assets, financing, acquisition, divestiture, or dissolution of all or a portion of our business.

- **Merchants.** Depending on the Services used by our Merchants, if you are an End Customer, we may share minimum data with the Merchant in order to provide our Services. We may share your data with other users of our Services with whom you interact through your own use of our Services to enable you to make or accept a payment using our Services.
- **Authorities**. We also disclose personal data to authorities to the extent we are under a statutory obligation to do so. Such authorities include tax authorities, police authorities, enforcement authorities and supervisory authorities in relevant countries. We may also be required to provide competent authorities information about your use of our Services, e.g. revenue or tax authorities, as required by law, which may include personal data such as your name, address and information regarding card transactions processed by us on your behalf through your use of our Services.
- We may also disclose information collected about you if (i) disclosure is necessary to comply with any applicable law or regulation, legal process or governmental request; (ii) to enforce applicable terms and conditions or policies; (iii) to protect the security or integrity of our Services; and (iv) to protect our rights (v) for an investigation of suspected or actual illegal activity; or (vi) to protect us, users of our Services or the public from harm, fraud, or potentially prohibited or illegal activities.
- **Where you ask us to share your personal data.** Where you direct us to share your personal data with a third party, we may do so. For example, you may authorise third parties to act on your behalf (such as a lawyer or accountant). We may need to ask for proof that a third party has been validly authorised to act on your behalf.
- We may also share aggregated information with third parties that does not specifically identify you or any individual.

Transferring information internationally

For our European business we store our personal data within the European Economic Area ("EEA"). We may transfer information collected about you to members of our group of companies, to parties who are part of the payment transactions process and third parties acting on our behalf that may be in countries outside

of the European Economic Area (“EEA”) or the United Kingdom to provide our Services. These other countries may not offer the same level of protection for the information collected about you, although we will at all times continue to collect, store and use your information in accordance with this Privacy Policy and the applicable data protection legislation. SumUp will ensure they share data only with those organisations that satisfy an adequate level of data protection in line with applicable data protection legislation and that satisfactory contractual agreements are in place with any such parties.

Cookies

We use cookies to analyse how you use our Website. Please read our Cookie Policy for more information about cookies. We also use pixels or web beacons in the direct marketing emails that we send to you. These pixels track whether our email was delivered and opened, and whether links within the email were clicked. They also allow us to collect information such as your IP address, browser, email client type and other similar details. We use this information to measure the performance of our email campaigns, and for analytics.

Linking to other websites

If you access links on our Website to third party websites which are not owned by SumUp please be aware that these websites have their own privacy policies. We do not accept any responsibility or liability for these privacy policies. If you visit such websites or use such services, please be aware that this Privacy Policy does not apply for such third parties’ processing, and we encourage you to carefully review how such third parties process personal data before using their websites or services.

Retention

We will not process personal data for a longer period than is necessary for fulfilling the purpose of such processing, as set out in this Privacy Policy. We store your information for as long as is necessary for the purposes identified in this Privacy Policy, including to provide our Services, to comply with legal obligations, to enforce and prevent violations of our Terms, to protect against fraudulent activity, and to defend our legal rights, property and users. Your personal data will be anonymized or deleted once it is no longer relevant for the purposes for which it was collected.

This means that we will only keep your data for as long as necessary for the performance of a contract and as required by applicable laws. If we keep your data for other purposes than those of the performance of a contract, such as anti-money laundering purposes, bookkeeping and regulatory capital adequacy requirements, we keep the data only if necessary and/or mandated by laws and regulations for the respective purpose.

The data retention obligations will differ within the SumUp Group subject to applicable local laws.

See below for examples of the retention periods that we apply:

- Preventing, detecting and investigating money laundering, terrorist financing and fraud: minimum five (5) years after termination of the business connection or if you receive services from our Lithuanian group companies eight (8) years from the date of termination of transactions or business relations with the client/last transaction.
- Bookkeeping, finance and accounting regulations: seven (7) years after the end of the financial year containing the latest date to which the information relates or ten (10) years as of the end of the corresponding financial year/last action under Lithuanian laws.
- Details on performance of an agreement: up to ten (10) years after end of customer relationship to defend against possible claims.

The above is only for explanatory purposes and the retention times may differ from country to country, the nature of the information and why it is collected

and processed and whether there is any related litigation, claim or complaint or regulatory matter.

Data security

We are committed to ensuring that the information collected about you is secure. We always process personal data in accordance with applicable laws and regulations, and we have implemented appropriate technical and organizational security measures to prevent your personal data from being used for non-legitimate purposes or disclosed to unauthorized third parties and otherwise protected from misuse, loss, alteration or destruction. The technical and organizational measures that we have implemented are designed to ensure a level of security appropriate to the risks that are associated with our data processing activities, in particular accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to your personal data including access control to premises, facilities, systems and data, disclosure control, input control, job control, availability control and segregation control. When you are logged into your account, all Internet communication is secured using Secure Socket Layer ("SSL") technology with high security 256bit encryption.

This high level of security can only be effective if you follow certain security practices yourself including never sharing your Account or login details with anyone. If you believe that any of your Account login details have been exposed, you can change your password at any time through our Website or mobile application, but you should always also immediately contact customer service.

Transmission of information via the Internet is not completely secure. Therefore, we cannot guarantee the security of the transmission of your information to us. Any transmission is at your own risk. Once we have received your information, we will use strict procedures and security structures to prevent unauthorised access.

SumUp is responsible for the security of cardholder data which is processed, transmitted and stored within our systems. To this end, SumUp is certified as compliant under the Payment Card Industry Data Security Standard (PCI-DSS).

SumUp applies best industry practice to safeguard this sensitive data and to ensure that it operates in line with these requirements, and to this end SumUp undergoes annual audits to ensure that we continue to meet this high standard.

Contact

You may contact us with your data protection queries at:

Email: DPO@sumup.com

Post:

SumUp Limited, Block 8, Harcourt Centre, Charlotte Way, Dublin 2, Ireland D02 K580

SumUp EU Payments, UAB, Upės str. 23, LT-08128, Vilnius

SumUp Payments Limited, 16-20 Shorts Gardens, London WC2H 9US, UK

Updates and notifications

We may change this Privacy Policy from time to time by posting the updated version on our Website. The “Last updated” legend at the top of this Privacy Policy indicates when this Privacy Policy was last revised.

Any changes are effective when we post the revised Privacy Policy on the Services. We advise you to review this page regularly to stay informed and to make sure that you are happy with any changes. If we make material changes to this Privacy Policy we will notify you by email or through posting a notification when you log into our Website or when you open our mobile application and/or Account/Profile.

If applicable law requires that we provide notice in a specified manner prior to making any changes to this Privacy Policy applicable to you, we will provide such required notice.

Language

The English language version of this Privacy Policy shall be binding. Any translation or other language version of this Privacy Policy shall be provided for convenience only. In the event of a conflict between the English version and any translation or other language version of this Privacy Policy, the English-language version shall prevail.