FreedomPay Privacy Policy
Version: 2.8
Date: August 29, 2022

I. Purpose

FreedomPay recognizes the importance of protecting your privacy and we work hard to safeguard your personal information. Our Privacy Policy is designed to assist you in understanding how we collect, use and store the information you provide to us when using any of our Services, regardless of how you use or access these Services.

This Privacy Policy will be updated or reviewed, at minimum, yearly. It is strongly recommended to check this document often.

Our Privacy Policy explains:

- What information we collect and its purpose
- How we obtain, process, disclose, share, retain and protect collected information
- The legal basis for processing collected data
- Your data protection rights regarding your information
- Who to contact regarding your data

II. Notice

Information We Collect

FreedomPay reserves the ability to share or permit access to personal information with persons we employ directly or as contractors or agents, partners, or affiliates at our direction, for purposes of administering our Services, processing information, marketing our Service and providing customer support. We share personal information with certain third parties such as the merchant of record, banks, processors, card networks, phone centers and other suppliers and vendors to provide the Services and to help us process the Services you request. FreedomPay requires such third parties to maintain confidentiality of your personal information.

Any information that can identify or reasonably link to, directly or indirectly, a consumer or household may be considered personal information. Anonymized data or data that is aggregated in such a way as to not be reasonably linkable with a specific consumer or household is not considered personally identifiable. FreedomPay reserves the ability to aggregate and disclose aggregated information that is not personally identifiable.

Generally, this aggregated information is used in statistical analysis. If FreedomPay sells all or substantially all of its assets, or completes a business transaction such as a merger, acquisition by a third party or a seal of all or a portion of our assets, this non-identifiable aggregated information may be one of the transferred assets.

Payment Gateway

FreedomPay's payment gateway solution securely collects and transmits credit card transaction data between merchants and processors. FreedomPay does not and will never store data defined as Sensitive Authentication Data (SAD), which includes CVV security code and PIN/PIN block and will only transmit that data as part of the credit card authorization process.

In addition to the collection and transmission of credit card transaction data, FreedomPay has the ability to collect certain information related to the transaction, including, but not limited to, name, address, occupation and email address. This information is provided to FreedomPay directly by the customer through a FreedomPay application, such as a credit application process, or through a FreedomPay partner that has integrated with a

FreedomPay application. Merchants may define additional data fields which relate to the transaction or may contain information provided by the customer and pass these data fields along with the transaction information to FreedomPay for analytical or record keeping purposes. The data that may be recorded falls under the following categories: identifiers, customer records information, commercial information, professional or employment-related information, and geolocation data.

Stored Value

FreedomPay's Stored Value platform is a white-label, closed-loop payment solution which is utilized for declining balance accounts or account-on-file recurrent billing. Stored Value funding options include automated and manual funding through bank accounts, credit/debit cards, and payroll deduction. Additional manual funding includes cash and check. For credit card transactions, FreedomPay utilizes FreedomPay's Payment Gateway to route and complete the transaction. Please refer to the Payment Gateway section for more detail surrounding credit card transaction data.

As part of the enrollment process to the Stored Value solution, FreedomPay collects information about to the Stored Value account holder, including, but not limited to name, address, occupation and email address. This information is provided to FreedomPay directly by the customer during the enrollment process, maintenance or modification of the customer account during the stored value account lifecycle, or through a FreedomPay partner that has integrated their existing stored value solution with FreedomPay. The data that may be recorded falls under the following categories: identifiers, customer records information, commercial information, professional or employment-related information, and geolocation data.

Business Intelligence Tool

FreedomPay's Business Intelligence Tool is a platform for providing customer intelligence via business reporting, containing trending, forecasting, market cluster/segmentation analysis. The scope of the data which will be loaded, analyzed, visualized, and made available to the end user through the Business Intelligence Tool is governed by the data being passed to

FreedomPay from the merchant environment. This data includes customer name, customer card number, and card type along with transaction and merchant specific information unrelated to the customers identity such as merchant address or location of transaction, currency type, and transaction totals. This data is combined with publicly available information (including demographic Census data, weather patterns, etc.) to generate additional ‘inferred’ or ‘derived’ data, to provide enhanced analytics throughout the merchant enterprise. The data that may be recorded falls under the following categories: identifiers, customer records information, commercial information, and geolocation data.

Corporate Website

HOTJAR

FreedomPay’s corporate website uses Hotjar in order to better understand our users’ needs and to optimize this service and experience. Hotjar is a technology service that helps us better understand our users experience (e.g. how much time they spend on which pages, which links they choose to click, what users do and don’t like, etc.) and this enables us to build and maintain our service with

user feedback. Hotjar uses cookies and other technologies to collect data on our users' behavior and their devices (in particular device's IP address (captured and stored only in anonymized form), device screen size, device type (unique device identifiers), browser information, geographic location (country only), preferred language used to display our website). Hotjar stores this information in a pseudonymized user profile. Neither Hotjar nor we will ever use this information to identify individual users or to match it with further data on an individual user. For further details, please see Hotjar's privacy policy by clicking on this link: https://www.hotjar.com/legal/policies/privacy You can opt-out to the creation of a user profile, Hotjar's storing of data about your usage of our site and Hotjar's use of tracking cookies on other websites by following this opt-out link: https://www.hotjar.com/legal/compliance/opt-out

LEADS AND MARKETING

FreedomPay also uses its corporate website to collect information provided by potential clients wishing to learn more about FreedomPay solutions. The information collected includes name, email address, phone number, state, postal code, country, job title and company name and is

used by our sales department for contact purposes to answer any questions regarding FreedomPay or the services we provide, and by our marketing department to distribute information regarding FreedomPay news, events, and webinars. This information is entered by the user through a form on our website and is imported into an internal management system for future communication. Once stored, this data may be shared with FreedomPay partners to assist potential clients with any additional questions they may have about all possible configurations of FreedomPay solutions. Individuals may unsubscribe from FreedomPay's marketing newsletters and webinar invitations at any time by clicking the unsubscribe link within the email, or by unsubscribing at the following link: https://pages.freedompay.com/UnsubscribePage.html

COOKIES

To improve your experience on our corporate website, FreedomPay utilizes 'cookies'. Cookies are an industry standard and most major web sites use them. A cookie is a small text file that our site may place on your computer as a tool to remember your preferences. You may refuse the use of cookies by selecting the appropriate

settings on your browser (refer to your browser or device help material), however please note that if you do this you may not be able to use the full functionality of this website.
Our website uses Google Analytics, a service which transmits website traffic data to Google servers in the United States. Google Analytics does not identify individual users or associate your IP address with any other data held by Google. We use reports provided by Google Analytics to help us understand website traffic and webpage usage. For more information on the cookies used by Google Analytics you can visit the following link: https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage
You may also opt out of Google Analytics by using the browser add-on at the following link: https://tools.google.com/dlpage/gaoptout/
For a full description of the cookies and services used within our website, please refer to the FreedomPay cookie policy, found here: https://corporate.freedompay.com/cookies-policy/

Employment Data

As an employer, FreedomPay collects personal information of its employees including name,

address, email, date of birth, bank information, work experience, and education history. This information is provided to FreedomPay by its employees through an application form distributed once an offer has been extended. We reserve the ability to share this information with third parties for the completion of background screenings, payment distribution, and enrollment in health/ financial benefits. FreedomPay requires such third parties to maintain confidentiality of employee personal information.

We release account and other personal information when we believe release is appropriate to comply with the law; protect the rights, property or safety of FreedomPay, our users or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction. Certain federal, state and local laws or government regulations may require us to disclose non-public personal information about you to respond to court orders or legal investigations. Note that this does not include selling, renting, sharing, or otherwise disclosing personally identifiable information from customers for

commercial purposes in violation of the commitments set forth in this Privacy Policy. We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.

Children's Notice

FreedomPay recognizes how important it is to protect the online privacy of children. FreedomPay's services are neither intended for children nor are they designed to attract child users. FreedomPay does not knowingly collect personal information from users under 18, would not willingly provide this data to any third party for any purpose, and any subsequent disclosure would be due to the user submitting personal information without solicitation from FreedomPay.

Contacting Us

In compliance with GDPR, and other various statutes, FreedomPay commits to resolve complaints about your privacy and our collection or use of your personal information. European Union or Swiss individuals with inquiries or complaints regarding their personal data that is

transferred into the United States should first contact FreedomPay at techsupport@freedompay.com.
If you have any questions about our Privacy Policy, would like to make a data request, or need to get in contact with our Data Privacy Officer, you may contact us in the following ways:
Email: compliance@freedompay.com
Website: https://corporate.freedompay.com/consumer-privacy/
Toll-Free Number: 1-888-495-2446

Independent Dispute Resolution

Data subjects under the jurisdiction of GDPR can file a complaint with the courts of the EU member state where they reside, where they work, or where the alleged infringement occurred.
If your complaint involves human resources data transferred to the United States from the EU [and/or Switzerland] in the context of the employment relationship, and FreedomPay does not address it satisfactorily, FreedomPay commits to cooperate with the panel established by the EU data protection authorities (DPA Panel) and the Swiss Federal Data Protection and Information Commissioner, and to comply with the advice

given by the DPA panel and Commissioner, with regard to such human resources data. To pursue an unresolved human resources complaint, you should contact the state or national data protection or labor authority in the appropriate jurisdiction. Contact details for the EU data protection authorities can be found at http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm
Contact details for the Swiss Federal Data Protection and Information Commissioner can be found at https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/links/data-protection—switzerland.html

III. Choice

As stated in II. Notice, Information We Collect, FreedomPay collects certain data that is required for performance of its Services. Separate from the performance of its Services, FreedomPay reserves the ability to aggregate and disclose aggregate data that is not personally identifiable to its partners or third parties. This aggregated, non-identifiable data will be used in statistical analysis or for other similar purposes.

For data defined as sensitive information, such as health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of an individual, FreedomPay must obtain written express consent from its customers or employees to share this data for any purpose outside of performing its Services. Please note, that FreedomPay does not collect this type of sensitive information as part of its Services, but this section has been included for transparency.

IV. Accountability for Onward Transfer

Transfer of Personal Information

Should FreedomPay enter into an agreement with a third-party organization acting as a controller, FreedomPay agrees that it will, to the best of its ability, require the third-party controller to agree to the terms listed in section II. Notice, III. Choice,

and V. Security, as well as meet the minimum security standards of FreedomPay including, but not limited to, PCI DSS compliance. As grounds for data transfers from the EU to third countries, FreedomPay relies upon Standard Contractual Clauses (SCCs), which set out appropriate safeguards for transfers of personal data. FreedomPay agrees to also require that, if entering into an agreement with a third-party controller, that the controlling entity be required to cease processing data that falls within scope of this privacy policy and/or take immediate steps to remediate should the determination be made that the entity is unable to abide by this policy. FreedomPay may be liable for the appropriate onward transfer of personal data to third parties. FreedomPay utilizes third party organizations as agents to perform its Services. These agents include:

- Processors
- Acquiring Banks
- Fraud management Providers
- Dynamic Currency Conversion Providers
- Chargeback Providers

For each of these providers, explicit consent must be received by the merchant as part of an overall agreement before this information can be shared.

FreedomPay agrees that for existing and future third-party agents assisting in performing services its services involving the sharing of personal data it will:

1. Transfer such data only for limited and specified purposes;
2. Contractually provide that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles;
3. Take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles;
4. Require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles;
5. Upon notice, including under (4), take reasonable and appropriate steps to stop and remediate unauthorized processing; and
6. Provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department of Commerce upon request.
7. Note that FreedomPay may be required to share personal data in response to lawful requests from public authorities including to meet national security and law enforcement requirements.

V. Security

FreedomPay transmits, processes and stores customer and employee data and takes

appropriate measures to protect this data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data. Annually, FreedomPay undergoes security audits which include, but are not limited to, Payment Card Industry Data Security Standard (PCI DSS), SSAE16/SSAE18 SOCII Type II, and Payment Card Industry Point-to-Point Encryption (PCI P2PE). As a service provider per PCI DSS standards, FreedomPay also undergoes regular security testing of its environment by independent 3rd party organizations to test the security of its environments. Upon request, FreedomPay will provide documented evidence of its compliance with relevant security standards. For questions or inquiries regarding FreedomPay's security and compliance requirements, please contact compliance@freedompay.com.

VI. Data Integrity and Purpose

FreedomPay's use of personal information and data collected from its customers and employees will be limited to data that is 1) required for satisfactory performances of its Services or 2) collected and utilized to enhance the user experience of the Services. FreedomPay limits the information that it collects to data that is relevant for the satisfactory delivery and performance of FreedomPay's Services and does not process personal information or data that is incompatible with its intended use as described above or as required by legal or regulatory bodies. FreedomPay's use of personal information is retained in an individual-identifiable form only so long as needed to perform its Services, as required by legal or regulatory bodies, or as needed for reasonable means such as statistical analysis. Following that period, stored data is aggregated and no longer identifiable to a specific transaction or user.

VII. Data Protection Rights

FreedomPay is obligated through several consumer privacy laws, such as but not limited to the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), to inform users about their rights as consumers in regard to their personal data. FreedomPay seeks to inform users about their rights in a clear and transparent way and create an environment where individuals can share their information whilst having the value of their privacy upheld. Your specific rights will be determined either by where your data is procured from, from your place of residence, or a combination of both.

For all users outside of GDPR and CCPA jurisdiction, FreedomPay will respond to user data access, deletion, or rectification requests and the time frames for those requests in compliance with the varying local, national, or regional data protection and privacy laws and regulations without undue delay. The time frame for FreedomPay's response to the consumer may be extended when additional reasonable verification of identify of the data subject is required, or if there are numerous or complex requests. FreedomPay will take every reasonable measure possible to

prevent unauthorized disclosures of personal information. In general, vexatious or otherwise malicious or excessive requests may be refused at FreedomPay's discretion.

GDPR

The European General Data Protection Regulation, which came into effect on May 25th, 2018, provides eight fundamental rights to any data subject, regardless of citizenship, located within the confines of the European Union. These rights are as follows:

- The right to be informed. FreedomPay seeks to be clear and transparent with user information and utilizes this Privacy Policy to communicate about data being collected, how the data is used, how long the data will be kept and the criteria determining this, and how data is processed. FreedomPay provides contact details of the data privacy officer within this document. FreedomPay seeks to inform users about their rights to ensure fair and transparent processing.
- The right to access. Consumers have the right to learn if data is being processed by FreedomPay, the business purpose of their processed data, the categories of data processed and stored, the time period for storage or the criteria used to determine this period, the source of stored data, any automated decision making regarding their information, the existence of the rights to request rectification, erasure, or restriction of processing of information, and the right to lodge a complaint with a supervisory authority. Where personal data is transferred to

a third country or to an international organization, FreedomPay has provided appropriate safeguards as required by Article 46 of GDPR through Standard Contractual Clauses.

- The right to rectification. Consumers may request that personal information that is inaccurate or incomplete regarding the data subject is updated without undue delay. FreedomPay allows consumers to exercise this right taking into account the purpose of processing the data being requested for rectification.
- The right to erasure. Consumers may request that FreedomPay erases personal data when their personal data is no longer necessary for the purpose of which it was collected, where there is no legal ground for processing, no legitimate grounds for processing, for compliance with legal obligations to which FreedomPay is subject, or when related to processing the information of children below the age of 16. FreedomPay allows consumers to exercise this right depending on the type of data being requested for erasure.
- The right to restrict processing. Consumers can request that FreedomPay limits the way they use their personal data and can be used as an alternative to the right to erasure when the user believes their data is inaccurate or for legal claims regarding the data.
- The right to data portability. Any data information provided by FreedomPay will be provided in a commonly used and machine-readable format. Consumers have the right to transfer their information to another controller, where technically feasible.
- The right to object. Consumers may object to the processing of their personal data being collected by FreedomPay in certain circumstances, such as for direct marketing purposes.

- Rights related to automated decision making. Consumers are permitted to challenge and request a review of data processing regarding automatic decision making.

As defined by GDPR, the data controller is the principal party collecting personal data from data subjects, who determines the purposes and means of the processing of personal data. Data controllers have the primary responsibility for managing consent and data requests.

Data processors process personal data on behalf of data controllers. FreedomPay is primarily a data processor. For example, if a merchant seeks to use FreedomPay's payment gateway to process credit card transactions, the merchant is the data controller while FreedomPay is the data processor.

Data subject access requests may be made directly to FreedomPay only where FreedomPay is the data controller. Data subjects looking to modify their consent, access or delete their data, or exercise any other right under GDPR must contact the data controller (merchant) in order to resolve their request. The data controller (merchant) will contact the data processor (FreedomPay) as necessary on behalf of the consumer to fulfill the data request.

Data subject requests can only be made by the data subject the personal data pertains to, or by an entity or individual entitled to act on behalf of the data subject. To prevent unauthorized disclosure, FreedomPay will make reasonable attempts at verifying the data subject requestor's identity, or the authority granted by the requestor on behalf of the data subject. Requests under GDPR will be replied to without undue delay within 1 month from the date of receipt but may be subject to extension for up to an additional 2 months depending on the number and complexity of requests. Extensions will be communicated and justified to the requester as soon as possible and within the initial 1-month deadline. Vexatious or otherwise malicious or excessive objections may be subject to reasonable charges or refused at FreedomPay's discretion. If FreedomPay does not comply with a request, FreedomPay will provide reasoning for non-compliance, and the requestor may seek an internal review of the decision, and subsequently make a complaint to their local Information Commissioner's Office, information on which can be found under section II. Notice, Contacting Us, Independent Dispute Resolution.

CCPA

The CCPA, which came into effect January 1st, 2020, provides California residents a number of consumer rights in relation to the collection and processing of their personal information. These rights are as follows:

- The right to access. FreedomPay seeks to be clear and transparent with consumer information and utilizes this Privacy Policy to communicate about the categories of consumer data being collected, the sources of consumer data collection, and the business purpose for collecting consumer information. Consumers may make requests to access personal information, and FreedomPay shall promptly take steps to disclose and deliver, free of charge, the consumers personal information held by FreedomPay. FreedomPay will provide this data to the consumer in a portable, readily usable format after successfully verifying the consumer's identity, and is not required to provide personal information to a consumer more than twice in a 12-month period. FreedomPay collects information during the card transaction process, through marketing initiatives, and our website.
- The right to request deletion. Consumers may request that their personal information may be deleted. Requests for deletion can only be made by the data subject the personal data pertains to, or by Authorized Agents acting on the individual's behalf. Requests will be replied to without undue delay but may be subject to extension depending on the number and complexity of requests, and only after

verification of the identity of the consumer or entity requesting deletion. Please see the notes on transaction data for specific exemptions on data deletion requests.

- The right to disclosure. Consumers have the categories of personal information collected about the consumer, the categories of sources from where the personal information is collected, the categories of third parties with whom the business shares personal information, the business purpose of collecting the consumer's data, and the specific pieces of personal information it has collected about the consumer. The information within this section shall be provided alongside any consumer data request upon successful verification of the consumer's identity. Requests for access can only be made by the data subject the personal data pertains to, or by Authorized Agents acting on the individual's behalf.
- The right to opt out. Consumers have the right to opt out to the sale of personal information to third parties. FreedomPay does not sell personal information, and as such has not sold personal information within the last 12 months.
- The right to non-discrimination. Consumers will not be discriminated against by FreedomPay if they choose to exercise their rights granted under the CCPA.

As defined by CCPA, a "business" qualifies for CCPA when they i) do business in the state of California, ii) collects personal information of California residents (or has such information collected on their behalf iii) determines the purposes and means of the processing of

consumers' personal information, and iv) satisfies the following:

- Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), adjusted for inflation
- Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices
- Derives 50 percent or more of its annual revenues from selling consumers' personal information.

Service providers process data on behalf of a business for a business purpose pursuant to a written contract which prohibits the service provider from retaining, using, or disclosing the personal information other than the specific purpose of performing the services specified in the contract for the business, or otherwise permitted by CCPA. FreedomPay is primarily a service provider. For example, if a merchant seeks to user FreedomPay's payment gateway to process credit card transactions, the merchant is the business while FreedomPay is the service provider.

Consumer access requests may be made directly to FreedomPay only where FreedomPay is the business. Consumers looking to modify their consent, access or delete their data, or exercise

any other right under CCPA must contact the business (merchant) in order to resolve their request. The business (merchant) will contact the service provider (FreedomPay) as necessary on behalf of the consumer to fulfill the data request.

Consumer requests can only be made by the consumer the personal data pertains to, or by an Authorized Agent registered with the California Secretary of State entitled to act on behalf of the data subject. To prevent unauthorized disclosure, FreedomPay will make reasonable attempts at verifying the consumer or Authorized Agent's identity. Requests under CCPA will be replied to without undue delay within 45 days from the date of receipt but may be subject to extension for up to an additional 90 days depending on the complexity and number of requests. Extensions will be communicated and justified to the requester as soon as possible and within the initial 45-day deadline. Vexatious or otherwise malicious, repetitive or excessive objections may be subject to reasonable administrative charges or refused at FreedomPay's discretion. The consumer will be

notified of such decisions, and FreedomPay will demonstrate the reasoning behind actions taken against any verified consumer request.

Transaction Data

FreedomPay acknowledges the individual's right to access the personal data we hold about them. Customers wishing to review, amend, or correct their personal data may do so by contacting the merchant that accepted the individual's payment card in payment for goods or services. If a customer contacts FreedomPay for this purpose, FreedomPay will direct that customer to contact such merchant. As a payment processor, FreedomPay provides its merchants access to customer transactional data, but only in truncated formats in an effort to protect customer data from potential breach or compromise. FreedomPay receives customer data through the normal credit card transaction payment process, and transmits, stores and processes transactional data to perform its services.

In general customers do not have access to the FreedomPay transaction processing system due to the security and regulatory requirements

required of payment processors. Providing customers access to their data introduces a disproportionate risk to both FreedomPay and the customer data, and therefore FreedomPay does not offer access to this highly sensitive data.

GDPR

Under GDPR, as this transaction data is being collected due to a legitimate interest and pursuant to the execution of contracts, FreedomPay is not required to delete, or modify transactional data in response to a data subject access request.

CCPA

Under CCPA, as this transaction data is needed to complete transactions for which it was collected, needed to provide goods or services requested by the consumer, required to perform a contract, and used in context of the business relationship with the consumer, FreedomPay is not required to honor deletion requests for transactional data.

Business Data

Potential or existing clients who wish to review, amend, or delete the contact information stored in FreedomPay's marketing and Customer

Relationship Management (CRM) platforms can submit a request at https://corporate.freedompay.com/consumer-privacy/. Following validation of the data subject, a member of the FreedomPay compliance team will execute the request and provide any accompanying documentation.

Human Resources Data

FreedomPay Employees wishing to review, amend, or delete their personal data may do so manually by accessing the appropriate HR web portals. Using these portals, FreedomPay employees have the ability to view and edit any information provided to the Human resources department. Some information may be stored in systems that do not offer an externally facing method for review, amendment, or deletion. In these instances, employees may contact FreedomPay's Director of Human Resources for assistance. Due to financial and legal requirements, as long as an individual is employed at FreedomPay, not all employee data can be

deleted without terminating the existing employment arrangement.

FreedomPay's subsidiary, FreedomPay World Europe Limited, located at 40 Bank ST., 26th Floor, Canary Wharf, London E14 5AB, United Kingdom, also adheres to the terms and principles of this privacy policy, including the use of personal data received from the EU. At this location, FreedomPay has designated its EU representative as SVP of Global Product Delivery, Tony Hammond as required by GDPR Article 27.