ConnectPay

Privacy Policy

Version effective 2022 04 12 – 2022 12 21

ConnectPay

Table of Contents

1. General Terms

1.1. Data Controller - UAB "ConnectPay", company code 304696889 (hereinafter – the Company), registered address at Algirdo str. 38, 03218, Vilnius, Lithuania. The Company is an electronic money institution authorized and regulated by the Lithuanian supervisory authority – Bank of Lithuania. The Company's activities include the issuing of electronic money, distribution and redemption of electronic money, issuing of payment instruments and/or acquiring of payment, execution of payments transactions, payment initiation, account information services. The license of the Company and all activities covered by it can be checked on the Bank of Lithuania's website here.

1.2. This Privacy policy sets out the basis on which the Company processes Customers' and Partners' personal data. This is further enforced by the Company's internal policies and procedures. All activities of the Company are regulated by the applicable laws related to electronic money, including, but not limited to all legal acts related to the financial institutions and financial services. Moreover, as the Company collects and uses the personal data (hereinafter – the Personal data) of its customers (hereinafter – the Customers), and third party service providers (hereinafter - Partners) the Company is obligated to use and process the Personal data of the Customers and Partners only in accordance with this privacy policy and the applicable acts which regulate the protection of Personal data.

1.3. When the Company's potential Customer is a legal person, the head or other representative of the Customer, filling out the registration application form for the use of the Company's products and services, shall properly inform the Data subjects (Beneficial owners, Head, etc.) about the transfer of their data to the Company, as well as the contents of the Company's Privacy policy.

1.4. Profiling by automated means may be used when processing Personal data for some services and products for the purposes of risk management in accordance with the Company's legal obligations as well as for internal assessment and analysis of the market products. When a decision is based on automated processing including profiling, you have the right to contact us and provide your objection to such a decision.

2. Principles of processing personal data

2.1. The Company commits to comply with the provisions of General Data Protection Regulation, the Law on Legal Protection of Personal Data of the Republic of Lithuania and other applicable Personal data protection regulations and legal acts in the Republic of Lithuania and the European Union.

2.2. This Privacy Policy is prepared for the purposes of introducing Customers and Partners to how the Company processes the Personal data of its Customers and Partners and what kind of measures are implemented in the Company to achieve the adequate protection of the Personal data that are processed during the provision of Services. The principles that the Company strictly follows to comply with the needs to protect its Customers' and Partner's Personal data are, as follows:

0. Personal data is collected for specified and legitimate purposes and will not be further processed in a way that is incompatible with those purposes established prior to the collection of Personal data.
1. Personal data is processed in a lawful, fair and transparent way.
2. Personal data is accurate and, if necessary for the processing of personal data, constantly updated.
3. Personal data is collected only to the extent which is necessary to fulfil the specified legitimate purpose.
4. Personal data is stored for the period specified by the Company, but not longer than the terms set forth by the applicable legal acts. When the storage term has expired, the Personal data will be destroyed.
5. Implementation of adequate organizational measures designed to secure Personal data against accidental or illegal destruction, modification, disclosure, and any other illegal management.
6. Implementation of measures designated for the prevention of the use of Personal data by persons seeking to acquire funds by fraudulent means.
7. The Personal data of the Customers and Partners is considered as confidential information and may only be disclosed to third parties in accordance with the rules and procedure provided in the Privacy Policy, internal documents of the Company and the legal acts of the Republic of Lithuania.

3. Legal basis for Personal data processing and purposes

3.1. Personal data is only processed by the Company when

- the customer has given consent
- processing of data is necessary in order to fulfill the Agreement to which the customer is a party or to take action at the request of the customer prior to the conclusion of the agreement
- to process data necessary for the fulfillment of the legal obligation imposed on the Company
- to process data based on Company's legitimate interest

3.2. The purposes of the processing of the Personal data are, as follows:

(a) The provision of any of the following Services:

· issuance, distribution and redemption of electronic money;

· execution of payment transactions;

· store money value service;

· payment initiation and account information service;

· corporate card service;

· individual card service;

· card acquiring service.

Legal basis of processing: performance of a contract.

(b) The conclusion and execution of agreements (with Customers or Partners)

Legal basis of processing: performance of a contract.

(c) Customer services, including responses to questions, feedback, complaints, and the provision of the information regarding the Company's products or services

Legal basis of processing: performance of a contract, legal obligation.

(d) Implementation of obligations under the Law on Money Laundering and Terrorist Financing Prevention and other applicable regulations (Customer's identification, verification of identity via live conference call, verification of customer's/ UBO's data against public registries, databases, public domain, etc., ongoing monitoring of the Customer's activity, risk assessment and analysis, risk management activities, inspections of the complex or unusually large transactions and unusual transaction structures)

Legal basis of processing: legal obligation.

(e) Implementation of obligations under regulations governing financial sector (e.g. due diligence of the 3rd party service providers as per EBA guidelines on outsourcing)

Legal basis of processing: legal obligation.

(f) Risk management processes (e.g. data processing for fraud prevention)

Legal basis of processing: legitimate interest - Company's interest to systematically monitor and prevent illegal acts and constantly assess related risks.

(g) Video surveillance in the physical office of the Company

Legal basis of processing: legitimate interest - Company's interest to protect employees, customers, potential customers, third parties and Company's property.

(h) Administration of data of potential customers, improvement of quality of the products and services

Legal basis of processing: legitimate interest - Company's interest of business development.

(i) Customer service quality assurance purposes and to protect customer's and the Company's interests.

Legal basis of processing: legitimate interest - Company's interest to monitor and ensure high quality standards and protect customers and Company from litigation processes.

(j) Debt management process

Legal basis of processing: legitimate interest - Company's interest to file and defend legal claims, and take other legal actions to avoid losses or reduce them.

(k) Additionally, the Company may collect and process the Personal data of the Customer as part of its direct marketing operations.

Legal basis of processing: consent of a data subject.

(l) On receipt of ad hoc data subject's request and proactive consent, their personal data may also be processed for the respective purposes specified in said request.

3.3. Personal data collected for direct marketing purposes may be processed only in those instances where the Customer has given clear consent for such actions. Consent can only be collected in a manner in which it is clearly indicated that the Customer agrees with the processing of their Personal data for the purposes of direct marketing. Direct marketing is all activities by which the Company offers its goods or services to the Customer by post, telephone or other direct electronic means. In the event that the Customer refuses consent to the processing of their Personal data for direct marketing purposes, their Personal data will not be processed for direct marketing purposes.

3.4. The Customer is granted the right to withdraw their consent given for the processing of the Personal data for the purposes of the direct marketing. The Customer may withdraw their given consent freely at any point of time by using the electronic channel which is dedicated to the management of the Customer's account and for the communication with the Company.

4. Types and Sources of Processed Personal data

4.1 In accordance with the purposes specified above in points a, b, c, d, e, f and j of the clause 3.2. the following Personal data is processed by the Company:

a) Customers (natural persons) - first name, surname, personal code, date of birth, place of birth, PEP status, nationality, age (year of birth), address, place of residence, identification card (passport) number, issuance place, date and expiry date, mobile phone number, email address, employment data, photo, signature, financial institution account number, IBAN number, debit card number, video and audio record for identification, telephone conversations, customer IP addresses, date of transaction, transaction amount, currency, location, data concerning the beneficiary of the funds, history of the actions performed, the source of funds, audio recordings if Customer calls to customer support, identity verification live video conference calls etc.;

b) Representatives of the Customers (natural persons or legal entities), members of the client's management bodies and other representatives (for example, employees) who are authorized according to corporate documents to represent the client in relations with the data controller or acting in accordance with power of attorney, or by official appointment for the purposes of representing the client): first name, surname, personal code, date of birth, place of birth, PEP status, nationality, age (year of birth), address, place of residence, identification card (passport) number, place of issuance, date and expiry date, mobile phone number, email address, employment data, photo, signature, bank account information (bank name and bank account number), date of transaction, transaction amount, currency, data concerning the beneficiary of the funds (natural person's name, surname, date of birth, personal identification number or other unique character assigned to this person to identify the person, legal entity name, legal form, registered office address, code, if any), audio recordings if data subject calls to customer support, identity verification live video conference calls, etc.;

c) Ultimate beneficiary owners of the clients (legal entities), natural persons who directly or indirectly own a legal entity with a sufficient number of shares or voting rights or otherwise exercise control: first name, surname, personal code, date of birth, place of birth, PEP status, nationality, age (year of birth), address, place of residence,

identification card (passport) number, place of issuance, date and expiry date, mobile phone number, email address, employment data, photo, signature, number of shares held, voting rights or share capital, date of transaction, transaction amount, currency, data concerning the beneficiary of funds (natural person's name, surname, date of birth, personal identification number, or other unique character assigned to this person to identify the person, legal entity name, legal form, registered office address, code, if any, bank account number), audio recordings if data subject calls to customer support, identity verification live video conference calls, etc.

d) Customers of the Merchants (natural persons using payment initiation or account information services): first name, surname, mobile phone number, email address, unique Merchant Consumer ID, IBAN number, IP address, audio recordings if data subject calls to customer support.

e) Customers of the Merchants (natural persons using card acquiring payment option): first name, surname, mobile phone number, email address, unique Merchant Consumer ID, IP address, masked card number, audio recordings if data subject calls to customer support.

f) Representatives of the Company's 3rd party providers, partners: first name, surname, mobile phone number, email address, audio recordings if data subject calls to customer support, video recordings of external training providers.

g) Individual Card holders and Corporate Card holders (natural persons, using CP corporate cards): first name, surname, personal code, date of birth, place of birth, PEP status, nationality, age (year of birth), address, place of residence, identification card (passport) number, place of issuance, date and expiry date, mobile phone number, email address, relationship with the Customer, account number for which card should be linked, card number, photo, signature, date of card transaction, transaction amount, currency, data concerning the beneficiary of the funds (natural person's name, surname, date of birth, personal identification number or other unique character assigned to this person to identify the person, legal entity name, legal form, registered office address, code, if any, bank account number), audio recordings if data subject calls to customer support, etc.

4.2. In accordance with the purposes specified above in point g of the clause 3.2. the following Personal data is processed by the Company:

Video footages of the individuals entering the physical office of the Company.

4.3. In accordance with the purposes specified above in point h of the clause 3.2. the following Personal data is processed by the Company: legal entity's representative's name, surname, position, phone number, email.

4.4. In accordance with the purposes specified above in point i of the clause 3.2. the following Personal data is processed by the Company: customer service audio calls recordings.

4.5. The Company has the right to process Personal data other than that specified, provided that legitimate and predefined objectives for the processing of Personal data are established. In this case, Personal data is collected and processed in accordance with the applicable legal requirements and procedures established by the competent authorities.

4.6. The Personal data collected and processed for the purposes of the direct marketing is as follows: name, surname, the email address, mobile phone number.

4.7. The Personal data of the Customer is kept in such a way that the identity of the Customer can be determined for no longer than is necessary for the purposes for which Personal data is processed. The terms of storage of the Personal data of the Customer for the purposes indicated in this Privacy Policy are set forth by the applicable law, or are set internally within the Company for the shortest time possible to achieve the set personal data processing purpose. The Company strictly follows those terms and in the event that changes appear, the terms will be altered in accordance with these changes. The Personal data of the data subject collected and processed for the purpose of direct marketing shall be kept for no longer than the consent of the Customer is valid.

4.8. The Personal data of the Customer/Partner is obtained from the following sources:

· the Customer or potential Customer - Personal data of the Customer (natural person) or Customer's (legal entity's) representatives is obtained at the beginning of the business relationship and may be further collected throughout the implementation of the contract;

· the Partner - Personal data of the partner's representatives is obtained at the beginning of the business relationship and may be further collected throughout the implementation of the service agreement;

· the commercial banks, or other credit and financial institutions - Personal data from commercial banks, other credit and financial institutions is obtained through execution of payment transactions;

· the Merchants - for payment initiation and account information services, Personal data is obtained from the Merchants, through the provision of payment initiation and/or account information service;

· other third-party providers such as state and non-state registers, public registers, databases for identity verification checks, international sanctions, law enforcement agencies, other databases and open-source engines. Personal data is obtained through the execution of such legal obligations as identification, due diligence processes, and required screenings.

5. Customer Personal data recipients

5.1. The Customer Personal data specified in this Privacy Policy may be transferred to:

a) payment service users (payees and payers);

b) financial institutions;

c) agent of a payment institution;

d) the Bank of Lithuania and the SEPA/International Interbank Financial Telecommunication System - SWIFT participant (personal data for these beneficiaries is subject to the use of the Single Euro Payments Area – SEPA/ SWIFT);

e) credit/debit card processing service provider;

f) identity verification service providers;

g) vendors of software development and support services;

h) transaction monitoring service providers;

i) risk management tools providers;

j) website domain hosting providers;

k) cloud service providers;

l) other suppliers;

m) law enforcement units, regulatory bodies, auditors or courts, in situations where the Company is required by law to do so.

5.2. Customer Personal data may be transmitted to third parties not specified above for specified and legitimate purposes only, and only to third parties who have the right established by laws and other legal acts to receive personal data in the countries of the European Union and the European Economic Area.

5.3. In some cases, the processing of Customer information described above may involve sending it to countries outside of the EEA. In such circumstances, the Company will take all reasonable steps to ensure that the Customer's data is treated securely and in accordance with this Privacy Policy.

6. Data Retention Period

6.1. We store the data for no longer than is required for the purposes for which the data is initially collected and processed.

6.2. Personal data records are stored for a maximum of 10 years after the termination of the business relationship with the Customer to comply with legal obligations and protect the Company's legitimate interests. Such records include Copies of the identity documents of a Customer, the identity data of a beneficial owner, the identity data of a beneficiary, direct video streaming/direct video broadcasting recordings, other data received at the time of establishing the identity of the Customer and account and/or agreement documentation.

6.3. Business correspondence with the Customer in paper or electronic form for 5 years from the date of termination of their business relationship with the Customer.

6.4. Consent for direct marketing is valid until such time as the Customer has withdrawn it or when the business relationship ends, but no longer than 5 years. For more detailed information on the specific retention periods applicable for other categories of personal data, please contact us directly via dpo@connectpay.com.

6.5. Partner's (outsourcing partners, correspondent banking partners and other 3rd party service providers) data is kept for 10 years after the partnership agreement expired.

6.6. Recorded phone calls, when data subject makes a call to CP customer support, are stored for up to 10 years after the recording date.

6.7. The Company's premises' entrance video recordings are kept for 60 calendar days.

6.8. In the event that the transaction was not concluded (no agreement is signed by both parties, business relationship is not started), Personal data of potential customers shall be kept for no longer than 2 years (due to 2 years limitation period for filing a complaint with the Data Protection Authority) from the date of receipt of the data, unless the Data subject has provided a written request for the destruction of the Personal data processed by the Company.

7. Security of personal data

7.1. The Company implements necessary organizational and technical measures to protect the Customers' personal data in transit and at rest from accidental or unlawful destruction, modification, disclosure, as well as any other unlawful handling.

8. Use of Cookies

8.1. Cookies are small text files, often including unique identifiers, which are sent by web servers to web browsers, and which may then be sent back to the server each time the browser requests a page from the server.

8.2. The Company has its own website, and cookies may be obtained in order to provide the Data subject with the full range of Services provided by the Company during website visits, and in order to improve the quality of the Services provided to the Data subject's computer (device). The Company may use the following types of cookies:

· Strictly necessary cookies - these cookies are absolutely essential for the website to function properly. These cookies ensure basic functionalities and security features of the website, anonymously. These cookies are mandatory and cannot be switched off.

· Functionality cookies —these cookies help to perform certain functionalities like sharing the content of the website on social media platforms, collect feedbacks, and other third-party features.

· Analytical cookies —these cookies are used to understand how visitors interact with the website. These cookies help provide information on metrics the number of visitors, bounce rate, traffic source, etc.

No sensitive personal information is collected through Google Analytics. None of this information can be used to identify or contact the Customer. It is all aggregated and, therefore, anonymized. Their sole purpose is to improve website functions. To find out about Google Analytics, click here. However, for Customers who still wish to opt out of Google Analytics cookies, more information can be found here.

· Performance cookies - these cookies are used to understand and analyze the key performance indexes of the website which helps in delivering a better usage experience for the visitors.

· Marketing cookies – advertisement cookies are used to provide visitors with relevant adds and marketing campaigns. These cookies track visitors across websites and collect information to provide customized adds.

8.3. List of cookies used by us currently:

Strictly Necessary Cookies		
Name	**Purpose**	**Expiry**

viewed_cookie_policy	To store whether or not the user has consented to the use of cookies. It does not store any personal data.	11 months
cookielawinfo-checkbox-necessary	To store user consent for the cookies in the category “strictly necessary”.	11 months
cookielawinfo-checkbox-non-necessary	To store user consent for the cookies in the non-necessary categories.	11 months
PHPSESSID	To store and identify a users' unique session ID for the purpose of managing user sessions on the website. The cookie is a session cookie and is deleted when all the browser windows are closed.	Expires When the browsing session ends.
connectpay.com-cookies-info	To check whether a user accepts cookie Policy or not.	When the browsing session ends.
cookielawinfo-checkbox-others	To store the user consent for the cookies in the category “Other”.	11 months
CookieLawInfoConsent	Records the default button state of the corresponding category along with the status of CCPA. It works only in coordination with the primary cookie, viewed_cookie_policy.contain values of both viewed_cookie_policy and cookielawinfo-checkbox-	1 year

	necessary/cookielawinfo-checkbox-non-necessary along with CCPA values.	
cookielawinfo-checkbox-advertisement	To record the user consent for the cookies in the category “Advertisement”.	11 months
cookielawinfo-checkbox-functional	To record the user consent for the cookies in the category “Functional”.	11 months
cookielawinfo-checkbox-performance	To store the user consent for the cookies in the category “Performance”.	11 months
cookielawinfo-checkbox-analytics	To store the user consent for the cookies in the category “Analytics”.	11 months
Analytical Cookies		
Name	**Purpose**	**Expiry**
_fbp	To store and track visits across websites.	24 Hours
_ga	Used to distinguish users.	2 years
_gat	To throttle the request rate to limit the collection of data on high traffic sites.	1 minute
_gat_gtag_UA_145907203_1	To store a unique user ID.	1 minute
_gid	To store information of how visitors use a website and helps in creating an analytics report of how well the website is performing. The data collected includes number of visitors, and	24 hours

	where those visitors have originated from.	
SAPISID	To collect user information for videos hosted by YouTube. An embedded YouTube-video collects visitor information and adjusted preferred settings. Google's tag management system uses this cookie to measure and improve the customer experience.	2 years
APISID	To measure the number and behavior of Google Maps users.	10 year
HSID	Cookies called 'SID' and 'HSID' contain digitally signed and encrypted records of a user's Google Account ID and most recent sign-in time. The combination of these cookies allows Google to block many types of attack, such as attempts to steal the content of forms that a Customer completes on web pages.	1 day or maximum of 2 years
SID	To authenticate users, prevent fraudulent use of sign-in credentials, and protect user data from unauthorized parties. For example, cookies called 'SID'	2 years

	and 'HSID' contain digitally signed and encrypted records of a user's Google Account ID and most recent sign-in time.	
SIDCC	To protect a user's data from unauthorized access.	2 years
SSID	To collect user information for videos hosted by YouTube.	2 years
SEARCH_SAMESITE	To prevent the browser from sending this cookie along with cross-site requests.	182 days
1P_JAR	To display personalized advertisements on Google sites, based on recent searches and previous interactions.	1 month
NID	To display personalized advertisements on Google sites, based on recent searches and previous interactions.	Session
OTZ	To help customize ads on Google properties, like Google Search.	1 month
Marketing Cookies		
Name	**Purpose**	**Expiry**
fr	To deliver, measure and improve the relevancy of ads.	3 months
test_cookie	To determine if the users' browser supports cookies.	15 minutes

IDE,DSID	One of the main advertising cookies on non-Google sites is named 'IDE' and is stored in browsers under the domain doubleclick.net. Another is stored in google.com and is called 'ANID'.	2 years
_Secure-3PAPISID , _Secure-3PSID , _Secure-3PSIDCC	Builds a profile of website visitor interests to show relevant and personalized ads through retargeting.	2 years
cb_anonymous_id	AdRoll user related.	1 year
cb_user_id	AdRoll user related.	1 year
cb_group_id	AdRoll user related.	1 year

8.4. The Customer has to express their consent or non-consent for the use of cookies. The cookies settings present the Customer with an overview of the cookie categories. The cookies (except for strictly necessary cookies) are used only when the Customer consents to their usage.

8.5. Delete stored cookies

8.5.1. If at a certain moment you have allowed the use of cookies when visiting our website and now you wish to opt out and delete the cookies collected, please find instructions on how to proceed according to your browser here.

9. Third Party Links

9.1. he company does not take any responsibility for any third-party links found in the Company's website and the privacy policies applied thereto.

10. Changes of this Privacy Policy

10.1. The Company may update this Privacy policy in case of changes in applicable legislation or changes in Company's operations. Updated Privacy Policy will be posted on this website. If updates reflect a substantial or material change to the Personal data processing, the Company will inform the Customer about this prior to these changes coming into effect.

11. The rights granted to the Customer as a personal data subject

11.1. In accordance with statutory regulations on data protection, the data subject has the right to access all Personal data relating to the Customer or Partner which has been collected or disclosed by the Company and a right to have such Personal data rectified in the event that such Personal data is inaccurate or incomplete. At any time, the Customer or Partner has the ability to exercise the following rights:

a) Right of access. The data subject has the right to obtain confirmation from the Company of whether or not personal data concerning him/her is being processed, and, where that is the case, access the said personal data.

b) Right of rectification. The data subject has the right to request that the Company rectify inaccurate Personal data concerning them, and they can also exercise their right to request that any incomplete Personal be completed. Please be advised that the Company may need to verify the accuracy of any new data the data subject provides to the Company.

c) Right to restrict processing. The data subject has the right to request that the processing of their Personal data be restricted provided that they can provide a legitimate reason. Where processing has been restricted, such Personal data shall, with the exception of storage, only be processed with the Customer's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or of a Member State.

d) Right to data portability. The data subject has the right to receive all Personal data concerning them that the data subject provided to the Company, and they also have

the right to transmit their data to another controller. Please be advised that this right only applies to information which the data subject provided to the Company.

e) Right of erasure (right to be forgotten). The data subject has the right to request that the Company erase all Personal data concerning them if there is no good reason for the Company continuing to process it. The Company may not, for specific legal reasons, always be able to comply with such requests. In such cases, the Company will inform the data subject of such inability at the time of the request.

f) Right to object. The data subject has the right to object at any time to the processing of Personal data concerning him/her which is processed for the purposes of the Company's legitimate interests.

g) Right to withdraw consent. The data subject has the right at any time to withdraw their consent for the Company's use of their Personal data. This will not, however, affect the legality of any processing that was carried out before data subject withdrew their consent. In some cases, in the event that the data subject withdraws their consent, the Company may not be able to provide the Services to data subject.

h) Right to submit application. The data subject has the right to submit applications directly to the State Data Protection Inspectorate (the supervisory authority of the Company for the protection of personal data) for any issues that arise in respect to the processing of personal data. The data subject may apply in accordance with the procedures for handling complaints that are established by the State Data Protection Inspectorate.

11.2. The Company undertakes to ensure that all other rights of the data subject as described in applicable laws are guaranteed to the Customer or Partner as a data subject.

11.3. The data subject can submit any inquiry regarding the processing of their personal data by contacting the Company via the contact information referred to in this Privacy policy. The Company undertakes to ensure that all information requested will be provided within 30 calendar days from the day the request was first received by the Company.

12. Contact the Company

12.1. The Company will be happy to help if any issues occur. Please contact the Company by sending an e-mail to our Data Protection Officer contact listed below.

Data Protection Officer

Email: dpo@connectpay.com

12.2. If you have any doubts or suspicions concerning the authenticity of any correspondence you have received from, or on behalf of, ConnectPay or its representatives, please contact CP immediately via any of the following contacts: by email: security@connectpay.com or by phone: +370 666 44600 I +356 279 22875