Effective as of 2025 09 15

Privacy Policy

- 1. General Terms
- 2. Principles of Processing Personal Data
- 3. Personal Data: Purposes, Categories, and Legal Basis
- 4. Sources of Personal Data
- 5. Personal Data Recipients and Transfers Outside the EEA
- 6. Data Retention Period
- 7. Security of Personal Data
- 8. Use of Cookies
- 9. Third Party Links
- 10. Changes of this Privacy Policy
- 11. Rights of the Data Subject
- 12. Contact the Company

---

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.

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, Heads, and other associated individuals) about the transfer of their data to the Company, and the processing

of such data in accordance with this Privacy Policy and applicable data protection laws. The Customer's representative must also provide access to this Privacy Policy to all relevant Data Subjects and ensure that any necessary consents or authorizations required under applicable law are obtained.

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. If we engage in automated decision-making that produces legal effects or similarly significantly affects you, we will ensure that you are informed, provided with meaningful information about the logic involved, and given the opportunity to express your point of view or contest the decision, as required by applicable law. Should you have any concerns or wish to inquire about automated decision-making or profiling, you may contact us at dpo@connectpay.com.

---

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:

1. 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.
2. Personal data is processed in a lawful, fair and transparent way, ensuring that individuals are informed of how their data is used.
3. Personal data is maintained accurately and updated as necessary to ensure its relevance and integrity for the purposes of processing.
4. Personal data is collected only to the extent necessary to fulfil the specified legitimate purpose.
5. Personal data is stored for the period specified by the Company to fulfill its purposes, but not longer than required by applicable legal obligations. Once the specified storage term expires, or the data is no longer needed, it will be securely deleted or anonymized.
6. Appropriate organizational and technical security measures are implemented to safeguard personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access or any other unauthorized or illegal processing.

7. Specific measures are in place to prevent the misuse of personal data by individuals or entities attempting to engage in fraudulent activities.
8. Personal data of the Customers and Partners is treated as confidential information. It may only be disclosed to third parties in accordance with the terms outlined in this Privacy Policy, internal documents of the Company and applicable legal requirements of the Republic of Lithuania.

---

3. Personal Data: Purposes, Categories, and Legal Basis

3.1. Personal data is processed by the Company on the following legal grounds:

- **Consent:** the data subject has provided clear and explicit consent.
- **Performance of a Contract:** processing is necessary to fulfill a contract to which the customer is a party or to take steps at the customer's request before entering into a contract.
- **Legal Obligation:** processing is required to comply with legal obligations imposed on the Company.
- **Legitimate Interest:** processing is necessary for the legitimate interests pursued by the Company, provided these do not override the interests or fundamental rights and freedoms of the data subject.

3.2. To ensure transparency and help you understand how the Company handles your personal data, the table below outlines the purposes for processing, the types of personal data involved, the categories of individuals to whom it applies, and the legal basis for each processing activity.

Purpose(s)	Data Subject(s)	Legal Basis	Data Categories	Data Provision

(1) Provision of Services (directly or through a Partner's Platform): • 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. **(2) Conclusion and Execution of Contracts:** to manage and fulfill agreements with customers or partners. **(3) Customer Services**: to respond to questions, feedback, and complaints, and to	• **Customers** (natural persons registering for the Company's services directly or through a Partner's Platform). • **Representatives of Customers** (natural persons or legal entities registering for the Company services directly or through a Partner's Platform, including members of the client's management bodies or other representatives (e.g., employees) authorized by corporate documents, power of attorney, or official appointment to act on behalf of the client. • **Ultimate Beneficial Owners (UBOs)**: natural persons who directly or indirectly own or control a legal entity registering for the Compnay	**Performance of a contract** (when the data subject is a party to a contract) **Legal obligation** (e.g., managing complaints as part of customer service, compliance with AML and CTF laws, adherence to financial sector regulations, such as conducting due diligence on third-party service providers, and other mandatory legal and regulatory requirements) **Legitimate interest** – the Company's interest in provision of services as part of its contractual relationships with corporate customers, which includes processing data of corporate	**Common data for Customers, Representatives of Customers, UBOs and Individual and Corporate Card Holders:** 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, identity verification video and audio record, IP addresses, date of transaction, transaction amount, currency, location, data concerning the beneficiary of	**(1) Provision of Services (accounts, cards, payments, etc.)**: providing this data is necessary to enter into and perform a contract with the Company for financial services. Without this information, the Company will be unable to provide services such as account opening, card issuance, or payment execution. **(2) Conclusion and Execution of Contracts:** provision of the relevant personal data is required to conclude and manage contractual relationships. If the data is not provided, the Company will be unable to offer, maintain, or terminate services in accordance with contractual obligations.

provide information about the Company's products and services. **(4) Compliance with Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) Laws**: to fulfill legal obligations, including customer identification, identity verification (e.g., via live conference calls), checks against public registries/databases, ongoing activity monitoring, risk assessments, and analysis of unusual transactions or structures. **(5) Compliance with Financial Sector Regulations**: to meet obligations under financial sector laws, such as conducting due diligence on third-party service providers (e.g., in line with EBA outsourcing guidelines).	services (directly or through a Partner's Platform) through a significant number of shares, voting rights, or other means of control. • **Individual and Corporate Card Holders** (natural persons, using Compnay corporate cards registering for Compnay services directly or through a Partner's Platform). • **Merchant Customers** (payment initiation and account information users) • **Merchant Customers** (card acquiring users) • **Company Partner's Platform Users** (natural persons or legal entities using the Platform services to send or receive payments without	representatives to fulfill contractual obligations. Additionally, the Company processes data for risk prevention and management, such as monitoring and preventing fraud, systematically assessing related risks, pursuing debt recovery, and protecting the Company's interests through legal recourse. **Legitimate interest** also serves as a legal basis **for processing 'silent party' data,** specifically to facilitate the execution of a contract with the payment service user and ensuring compliance with legal and regulatory requirements, such as AML/CTF laws.	the funds (natural person's name, surname, date of birth, personal identification number or another unique identifier assigned to the individual, legal entity name, legal form, registered office address, code, if any), history of the actions performed, the source of funds, audio recordings if data subject calls to customer support, and similar. **Additional data to UBOs only:** number of shares held, voting rights or share capital. **Additional data to Individual and Corporate Card Holders only:** relationship with the customer, the account number to which the card is linked, and the card number.	**(3) Customer Services: p**roviding contact and (1) support-related data is necessary to respond to service-related requests or complaints and may be required to fulfil pre-contractual or contractual obligations. Without such data, the Company may be unable to respond or resolve issues effectively. **(4) Compliance with AML and CTF Laws: providing** personal data for AML/CTF purposes is a legal obligation under applicable financial crime prevention laws. If the required data is not provided, the Company will be unable to establish or continue a business relationship.

(6) Risk Management: to process data for fraud prevention and systematically monitor and mitigate risks related to illegal activities. **(7) Debt management:** to file and defend legal claims and take other legal actions necessary to mitigate or prevent financial losses.	registering for the Company services). • **"Silent parties"** (individuals who are not direct users of the Company's payment services but whose personal data is processed because they are involved in transactions with the Company's payment service users. For example, if a customer of the Company sends or receives money from another person, the Company may process that other person's (the silent party's) data to complete the transaction). • **Representatives of the Company's Third-Party Providers and Partners**		**Specific to Merchant Customers: Payment Initiation and Account Information Users**: 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. **Specific to Merchant Customers: Card Acquiring Users:** 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. **Specific to Company Partner's Platform Users:** data	**(5) Compliance with Financial Sector Regulations:** the provision of personal data in this context is mandated by financial supervisory and regulatory frameworks. Without the required data, the Company may be prohibited from entering into or maintaining partnerships or service agreements under applicable law. **(6) Risk Management (including fraud prevention and monitoring):** there is no legal or contractual obligation to provide personal data for this purpose. However, processing is based on the Company's legitimate interest in ensuring secure and compliant service use. If

			collected may vary based on the individual's actions on the Platform. For payment execution purposes, basic information such as first and last names, contact details, and payment instrument details may be collected. Additionally, transactional data (e.g., payment order details), IP address, and other technical information specific to the Platform's setup are collected during payment execution. **Specific to "Silent Parties":** name, surname (if available and necessary for transaction processing), account number (e.g., IBAN or other unique account identifiers), transactional data (transaction amount, date of	such data is not provided or collected, the Company may be unable to offer or continue services in a secure and lawful manner. **(7) Debt Management:** provision of relevant personal data is necessary to fulfil contractual obligations and to support the Company's legitimate interest in recovering debts. Without this data, the Company may be unable to enforce claims or resolve outstanding balances.

			the transaction, transaction description or purpose (if included in the payment)), the role of the silent party in the transaction (e.g., payer, payee). **Specific to Representatives of the Company's Third-Party Providers and Partners**: first name, surname, mobile phone number, email address, audio recordings (if data subject contacts customer support), and video recordings of external training providers' sessions).	

Safety and Security (Video Surveillance)	Individuals entering the Company's physical office	Company's legitimate interest in ensuring the safety of employees, visitors, and assets within its premises.	Video footage (specific to individuals entering physical premises).	While there is no legal or contractual obligation to provide personal data for this purpose, video surveillance is conducted based on the Company's legitimate interest in ensuring safety and security. Personal data is collected automatically when individuals enter monitored areas. If a data subject does not wish to be recorded, access to those areas may not be possible.

Customer Relationship Development	Representatives of potential customers	Company's legitimate interest in identifying and fostering relationships with potential customers to support business growth.	Name, surname, position, phone number, email address.	There is no legal or contractual obligation to provide personal data for this purpose. The Company may collect publicly available business contact details or other professional information based on its legitimate interest in developing potential customer relationships in a B2B context. Data subjects are not required to respond and may object to such processing at any time, in which case their data will no longer be used for this purpose.

Customer Service Quality Assurance and Dispute Resolution	Customers and other individuals communicating with the Company.	Company's legitimate interest in maintaining high service standards and resolving potential disputes effectively.	Audio recordings of customer service calls.	There is no legal or contractual obligation to provide personal data specifically for quality assurance purposes. However, customer service interactions may be recorded or logged based on the Company's legitimate interest in monitoring service quality and ensuring proper dispute resolution. If a data subject objects to such processing, the Company may be limited in its ability to improve service delivery or address service-related concerns effectively.

Direct Marketing	Customers and other direct marketing recipients who have provided explicit consent for direct marketing activities. Existing customers who qualify under the soft opt-in exception, as per the Lithuanian Electronic Communications Law, where marketing communications relate to similar products or services and an opt-out option is provided.	**Consent** (for new customers and other individuals) **Legitimate interest** (for existing customers under the soft opt-in exception).	Name, surname, email address, mobile phone number.	Provision of personal data for direct marketing purposes is voluntary. In cases where consent is required, marketing communications will only be sent if the data subject has provided valid consent, which may be withdrawn at any time. In other cases, data may be processed based on the Company's legitimate interest in promoting its services, in which case data subjects have the right to object. There are no consequences for choosing not to provide data or for withdrawing consent, apart from not receiving marketing content.

Ad Hoc Processing Requests: specific data processing activities carried out by the Company based on a direct request from the data subject. Such requests may include actions like processing data for a specific purpose defined by the individual, provided explicit consent is given at the time of the request.	Customers, Representatives of Customers or any other individuals who interact with the Company	The legal basis depends on the nature of the request. Processing may be carried out to comply with a **legal obligation** (e.g., when responding to regulatory authorities or data subject rights requests), **to perform a contract** (e.g., fulfilling client-specific service actions), or based on the Company's **legitimate interest** in managing operational or business inquiries. In limited cases, where the data subject voluntarily provides personal data unrelated to any legal or contractual requirement, processing may be based on **consent**.	Personal data categories depend on the specific request and may include any relevant data necessary to fulfill the purpose, such as name, contact details (email, phone), and additional data explicitly provided by the data subject in their request.	Provision of personal data in response to ad hoc requests depends on the nature of the request. Where required to fulfil a legal obligation or contractual duty, the data must be provided to allow the Company to comply or respond. In other cases, data may be processed based on the Company's legitimate interest in managing such inquiries. Failure to provide relevant data may result in the Company being unable to respond to or act on the request.

Public Acknowledgment and Event Highlights: to share images and information that recognize partnerships, highlight cooperation, or showcase event participation on the Company's website, social media accounts, and other online platforms.	Representatives of partner organizations (e.g., employees)	**Consent:** for posts including citations, names, and positions of partner representatives, explicit consent is obtained to ensure voluntary and informed participation. **Legitimate Interest:** for posts featuring only images without citations, names, or positions, the Company relies on its legitimate interest in acknowledging partnerships and promoting activities. In such cases, individuals are informed orally before publication and given the opportunity to object.	Photographs, names and positions (if included alongside citations).	Providing personal data for public acknowledgment is voluntary. Where posts include citations, names, or positions, explicit consent is required and may be withdrawn at any time. For posts featuring only non-identified images (e.g., event photography), personal data may be processed based on the Company's legitimate interest in promoting its activities and partnerships. In such cases, individuals are informed in advance and given the opportunity to object. If personal data is not provided or consent is withheld, the individual will not appear in related communications or publications.

3.3. **Direct Marketing and Consent.** Personal data collected for direct marketing purposes will only be processed with the Customer's explicit consent, except in cases where the **soft opt-in exception** applies, as outlined in the Lithuanian Electronic Communications Law. This exception allows the Company to send marketing communications to existing customers regarding similar products or services, provided they were given an opportunity to opt-out at the time of data collection and in every subsequent communication.

3.4. Consent must be obtained in a clear and transparent manner, ensuring the Customer understands and agrees to the use of their personal data for direct marketing activities. Direct marketing includes activities where the Company offers its goods or services via post, telephone, or other direct electronic means. If the Customer does not provide consent, or opts out, their personal data will not be processed for direct marketing purposes.

3.5. **Right to Withdraw Consent**. Customers have the right to withdraw their consent for direct marketing at any time, or to opt-out of receiving marketing communications under the soft opt-in exception. Withdrawal or opt-out can be done freely and easily through the electronic channel dedicated to managing the Customer's account and communication with the Company.

---

4. Sources of Personal Data

4.1. The Company collects personal data from a variety of sources to fulfill its contractual, legal, and operational obligations. These sources include:

- **Customers or Potential Customers:** personal data of natural persons or representatives of legal entities is collected at the start of the business relationship and may be further collected throughout the contract's implementation.
- **Partners:** personal data of partner representatives is collected at the initiation of the business relationship and may be further collected throughout the execution of the service agreement.
- **Commercial Banks and other Credit or Financial Institutions:** personal data is collected through the execution of payment transactions involving commercial banks or other credit and financial institutions.
- **Merchants:** for payment initiation and account information services, personal data is collected from merchants during the provision of these services.
- **Partner Platforms:** when customers register for Company services via a Partner's platform, personal data is collected directly from the Partner's platform through integrated APIs.
- **Third-Party Providers and External Databases:** personal data is obtained from state and non-state registers, public registers, databases used for identity verification checks, international sanctions lists, law enforcement agencies, and other databases and open-source engines. This is done to meet legal obligations, including identification, due diligence, and required screenings.

- **Publicly Available Sources:** in some cases, personal data may be collected from publicly accessible information, such as company websites or public directories, to support contractual or compliance-related activities.
- **Authorized Third Parties:** data may also be received from authorized third parties acting on behalf of the customer or partner (e.g., legal representatives, agents, or intermediaries).

---

5. Personal Data Recipients and Transfers Outside the EEA

5.1. The Company may share your personal data with the following categories of recipients to fulfill our contractual, legal, and operational responsibilities:

- **Payment Service Users:** payees and payers involved in payment transactions.
- **Financial Institutions:** banks and other financial institutions processing payments.
- **Agents of Payment Institutions:** authorized agents acting on behalf of payment institutions.
- **Central Banks and Payment Systems:** organizations like the Bank of Lithuania, SEPA (Single Euro Payments Area), or SWIFT (International Interbank Financial Telecommunication System) participant to ensure secure and efficient payment processing.
- **Card Processing Providers:** credit and debit card service providers.
- **Platform Partners and Participants:** partners operating the platform you are using, and where relevant, other platform participants.
- **Identity Verification Providers:** companies that assist in verifying your identity as part of legal and regulatory requirements.
- **Software Development and Support Vendors:** providers offering technical support, development, and maintenance for technical systems used by the Company.
- **Transaction Monitoring Service Providers:** vendors assisting with monitoring transactions for compliance, security, and fraud prevention.
- **Risk Management Tool Providers:** providers offering tools for risk assessment and fraud prevention.
- **Web Hosting and Domain Service Providers:** vendors managing the Company's website and associated domains.
- **Cloud Service Providers:** providers offering secure cloud storage and data processing services.
- **External Auditors and Consultants:** independent consultants or auditors, subject to confidentiality commitments.
- **Legal and Regulatory Authorities:** law enforcement agencies, courts, regulatory and administrative bodies, where required by law.
- **Insurance Providers:** if applicable, personal data may be shared with insurance providers for risk coverage and claims management.

- **Other Suppliers:** third-party suppliers providing goods or services essential to the Company's operations.

5.2. The Company may transfer your personal data to countries outside the European Economic Area (EEA), such as the United States or other locations where the Company or its service providers operate. These transfers are always conducted with strict safeguards to ensure your data is protected:

5.2.1. **Transfers to the USA:** if the recipient in the USA is certified under the EU-U.S. Data Privacy Framework (DPF), the Company relies on this framework to ensure compliance with EU data protection standards. If the recipient is not certified under the DPF, the Company uses Standard Contractual Clauses (SCCs) approved by the European Commission to protect your data.

5.2.2. **UK Transfers:** for data involving individuals in the UK, we apply SCCs supplemented by the UK Addendum issued by the Information Commissioner's Office (ICO) or, where necessary, the UK International Data Transfer Agreement.

5.2.3. **Transfers to Other Countries:** for transfers to countries outside the EEA, such as India or other locations, that do not have an adequacy decision, the Company ensures that appropriate safeguards, such as SCCs, are in place to maintain a high level of data protection.

5.3. If the legal frameworks used for data transfers (e.g., SCCs or the EU-U.S. DPF) are invalidated or restricted by courts or regulators, the Company will adopt alternative, legally compliant safeguards to protect your data.

---

6. Data Retention Period

6.1. We store personal 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 data subject has withdrawn it or when the business relationship ends, but no longer than 5 years.

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 the Compnay 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. If a contractual relationship has not started (i.e., no contract is signed), personal data will typically be stored for a maximum of 2 years from the date of receipt. During this period, the data subject may request the deletion of their personal data at any time. Upon receiving such a request, the Company will delete the data unless retention is required to meet compliance or regulatory obligations, such as addressing identified risks related to money laundering, fraud, reputational concerns, or other legal requirements. In situations where the contract is not signed due to identified compliance or regulatory risks, personal data may be retained for up to 8 years to ensure adherence to legal and regulatory obligations.

6.9. For more detailed information on the specific retention periods applicable for personal data, please contact us directly via dpo@connectpay.com.

---

7. Security of Personal Data

7.1. The Company implements necessary organizational and technical measures to protect 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, refer to Google website. However, for Customers who still wish to opt out of Google Analytics cookies, refer to Google tool for more information.

· 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. A detailed list of cookies currently in use is displayed on the cookie banner on the website.

8.4. Visitors can manage their cookie preferences using the cookie settings available on the website. These settings provide an overview of cookie categories and allow visitors to consent to or decline the use of non-essential cookies. Cookies other than strictly necessary cookies are only activated after explicit consent is provided.

8.5. **Deletion of stored cookies.** If you have previously allowed the use of cookies while visiting our website but now wish to opt out and delete the cookies stored on your device, please refer to the instructions provided for your specific browser at ABOUT COOKIES .

---

9. Third Party Links

9.1. The 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. Rights of the Data Subject

11.1. In accordance with applicable data protection laws, all data subjects are entitled to specific rights regarding the processing of their personal data. These rights ensure transparency, control, and the ability to address any concerns related to the handling of personal data. Data subjects may submit requests to exercise their rights by contacting the Company using the contact information provided in this Privacy Policy. The Company will ensure that all requests are addressed promptly and in accordance with statutory timelines. The Company is committed to facilitating the exercise of 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 lodge a complaint with a supervisory authority. If the data subject believes that their personal data has been processed unlawfully or that their rights under applicable data protection laws, including the GDPR, have been violated, they have the right to lodge a complaint with a supervisory authority. The supervisory authority responsible for overseeing the Company's compliance is the State Data Protection Inspectorate of Lithuania. Alternatively, you may choose to lodge a complaint with the supervisory authority in your country of residence or workplace within the European Union or European Economic Area.

11.2. The Company is committed to ensuring that all rights of data subjects, as provided under applicable laws, are fully respected and upheld.

11.3. Data subjects may submit inquiries or requests regarding the processing of their personal data by contacting the Company using the contact details provided in this Privacy Policy. The Company will ensure that requested information is provided within 30 calendar days from the date the request is received.

---

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.

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 the Company immediately via any of the following contacts: by email: security@connectpay.com or by phone: +370 666 44600 / +356 279 22875