Privacy Policy

1. Introduction

1.1. This Privacy Policy establishes basic principles on Personal data processing of VIA Payments UAB (hereinafter -VIALET).

1.2. The respective Policy is applicable if a Customer uses, has used or has intention to use financial services provided by VIALET, including the relationship with the Customer established before this Policy enters into force.

2. For the purpose of this policy the following definitions are used

2.1. **App** - a mobile software linked with Customer's account installed and used in mobile devices which belongs solely to the Customer.

2.2. **Customer** – any private individual who uses, has used or has expressed a wish to use or is in other way related to any of the services provided by VIALET. For the purposes of this Policy this Customer definition also includes any private individual such as the representative, beneficial owner, manager, board member or member of the management body of the company, whose Personal data is collected and processed by VIALET.

2.3. **Personal data** - means any information relating to an identified or identifiable Customer.

2.4. **Processing** - any operations carried out with Personal data (incl. collection, recording, storing, alteration, grant of access to, making enquiries, transfer, etc.).

2.5. **VIALET** - Via Payments UAB, company's registration code: 304531663, operating under the brand name "VIALET" with registered office at Konstitucijos pr. 7, Vilnius, the Republic of Lithuania, the electronic money institution license No.: 16, email: info@vialet.eu and which is acting as a Personal data controller.

3. General provisions

3.1. This Policy describes general principles on how VIALET processes Personal data. Specific details on the processing of Personal data might be also included in agreements entered or to be entered between the Customer and VIALET.

3.2. VIALET ensures, within the framework of applicable law, the confidentiality of Personal data and has implemented appropriate technical and organizational measures to safeguard Personal data from unauthorized access, unlawful Processing or disclosure, accidental loss, modification or destruction.

3.3. VIALET securely stores and processes Customer data in a secure manner in the EU unless other VALET conditions provide for a different location.

3.4. VIALET uses authorized processors for Personal data Processing. In such cases VIALET takes needed steps to ensure that such data processors process Personal data under the written instructions of VIALET and in compliance with applicable law and requires adequate security measures.

3.5. If Customer fails to provide VIALET with Personal data that is necessary for the conclusion and/or performance of an agreement or provision of VIALET services whereof is required by law or under the agreement, VIALET may be unable to provide services to Customer.

3.6. VIALET may use various technologies to collect and store information when Customer visits VIALET web page, and this may include using cookies or similar technologies to identify Customer's browser or device. VIALET's Cookies Policy is available on the VIALET website.

4. Categories of personal data

4.1. Personal data categories which VIALET processes are the following:

4.1.1. **Identification data** such as name, surname, personal identification code, place and date of birth, citizenship, data regarding the identification document (such as copy of the passport, ID card, date and country of issue, expiration date, document number, issuance authority), photo, signature;

4.1.2. **Contact data** such as phone number, email address, the residence address, language of communication;

4.1.3. **Financial data** such as account number, cash flow, i.e. incoming and outgoing payments and information included thereof, transaction history, loan obligations and other obligations, accounts held at other financial institutions;

4.1.4. Information relating to Customer **tax residence** such as country of residence, country of tax residence, taxpayer identification number (TIN), citizenship;

4.1.5. **Family data** such as information about Customer's family, heirs and another related person's;

4.1.6. **Professional activity data** such as Customer place of work, profession, position, occupation, length of service and education;

4.1.7. **Communication data** collected when the Customer communicates with VIALET via telephone, visual and/or audio recordings, e-mail, messages and other communication channels such as social media; data related to the Customer's visit at VIALET web page or communicating through other VIALET channels (such as chat).

4.1.8. **KYC data** such as data about the Customer' due diligence, incl. the relationships with legal entities for the execution of transactions on behalf of the legal entity, legal representatives (acting with relevant authorization or on any other basis), contracting parties and contract participants, funds and wealth sources, ultimate beneficial owners (UBO), general manager of a company; shareholder, amount of shares owned; member of the management board or any other management body; self-declaration of politically exposed person (PEP); information publicly available in public registers, social networks and other media, information obtained in screenings against sanction lists, PEP status; data on origin of assets such as source of funds (salaries, dividends, inheritance, investment income), source of wealth (ownership of businesses, property, long-term investments; Transaction partner data, including legal name and business registration data, nature and purpose of the relationship, jurisdiction of operation and incorporation; Connections to high-risk jurisdictions: Involvement in high-risk sectors, adverse media reports indicating possible criminal behavior or reputational risk, discrepancies between declared sources of wealth and actual financial behavior, internal risk assessments or justification for KYC risk rating;

4.1.9. Data related to the **services and service use data** the Customer received from VIALET such as the performance of the agreements or the failure thereof, executed transactions, usage of ATMs, concluded and expired agreements, submitted applications, requests and complaints, interests and service fees;

4.1.10. Data obtained from **public** registers and/or created while performing an obligation arising from law or resulting from enquiries made by investigative bodies, notaries, central tax administrator, courts and bailiffs, details of income, credit commitments, property holdings, and debt balances;

4.1.11. **Location data** such as Internet Protocol (IP) address, Handset ID or data processed on an electronic communications network or processed by means of electronic communications services, indicating the location of the electronic communications terminal equipment, including the location of the terminal equipment (address), connection point address.

5. Purposes and basis of processing personal data

5.1. VIALET processes Personal data only for specific and necessary purposes:

5.1.1. To enter into and perform an agreement in order to provide the respective service to the Customer;

5.1.2. For VIALET to perform the legal obligation;

5.1.3. Based on Customer consent to process Personal data for a specific purpose;

5.1.4. To implement the legitimate interests of VIALET or third party in order to provide the service specified in the agreement, ensuring the legitime interest arising from the legal enactments assessing whether the VIALET or third-party interests to process Personal data are proportionate to Customer rights to privacy.

5.2. VIALET process Personal data primarily to:

5.2.1. Provide the Customer with our services, for example:

5.2.1.1. To take steps at the request of the Customer prior to entering into an agreement, as well as to conclude, execute and terminate an agreement with VIALET;

5.2.1.2. To execute national and international transactions via credit institutions, settlement and payment systems;

5.2.1.3. For managing Customer relations, providing and administering access to the services.

5.2.2. For VIALET to perform the legal obligations, for example:

5.2.2.1. To inform the Customer about changes in the Processing of Personal data;

5.2.2.2. To process the requests and complaints received from Customer;

5.2.2.3. To check and verify the Customer's identity and to keep Personal data updated and correct by verifying and enriching data through external and internal registers (KYC);

5.2.2.4. To prevent, discover, investigate and report potential terrorist financing, money laundering and/or other financial crimes;

5.2.2.5. To comply with rules and regulations relating to accounting, responsible lending, tax and lending information exchange and risk management;

5.2.2.6. To carry out credit - and other risk assessments when providing credits and other services, risk hedging and capital requirements for VIALET;

5.2.2.7. To execute the requests of the investigation and other law enforcement agencies, courts, sworn bailiffs and other state institutions and officials specified in laws.

5.2.3. VIALET will in some cases ask for the Customer's consent to process Personal data. The consent will contain information on that specific processing activity. VIALET, for example, processes Customer's Personal data for direct marketing purposes based on Customer's consent. Consent can always be withdrawn, and the Customer will be informed of any consequences of such withdrawal;

5.2.4. For the implementation of the VIALET or third party's legitimate interests, for example:

5.2.4.1. To offer and provide the Customer additional services or services of carefully chosen partners, create personalized offers;

5.2.4.2. To develop, examine and improve VIALET business, the services and the Customer's user experience by performing surveys, analyses, statistics;

5.2.4.3. To organize campaigns for the Customers;

5.2.4.4. To protect the interests of the Customer and/or VIALET employees, including security measures;

5.2.4.5. To manage the relationships with the Customer;

5.2.4.6. To prevent, limit and investigate any misuse or unlawful use or disturbance of the services;

5.2.4.7. To ensure adequate provisions of the services, the safety of information within the services, as well as to improve, develop and maintain applications, technical systems and IT-infrastructure, including testing VIALET's digital environment;

5.2.4.8. To carry out credit- and other risk assessments when providing credit and other services to natural person or legal entity; to manage the relationships;

5.2.4.9. To establish, exercise and defend legal claims.

6. Providers and recipients of personal data

6.1. Personal data is obtained:

6.1.1. when the Customer provides it to VIALET:

6.1.1.1. While applying for and using products and services;

6.1.1.2. While addressing VIALET by mail, email, over the phone, using chats and other communication channels;

6.1.1.3. While providing information relating to payments;

6.1.1.4. While visiting VIALET homepage and using mobile application, i.e. Customer profile and use data, how Customer uses these services, obtaining information from Customer's devices – computer, mobile telephone, with the help of cookies or Internet monitoring software (more detailed information is available in the Cookie Policy).

6.1.2. When third parties provide it to VIALET:

6.1.2.1. Third parties that provide to VIALET information relating to the Customer, conduct market research;

6.1.2.2. Database maintenance companies, registers;

6.1.2.3. State institutions and law enforcement agencies and officials thereof;

6.1.2.4. Persons in relation to contracts and transactions which these persons intend to conclude or have concluded with VIALET.

6.1.3. When VIALET collects this information from:

6.1.3.1. Other financial institutions;

6.1.3.2. Official and public registers, social media;

6.1.3.3. Legal entities, in respect to their representatives, employees, contractors, founders, shareholders, participants, owners, etc. of such legal entities.

6.2. Personal data is shared with other recipients (data processors or controllers or joint controllers), such as:

6.2.1. Counterparties (processors or separate controllers) related to the provision of the services and which VIALET has thoroughly assessed prior to cooperation;

6.2.2. Other credit and financial institutions, payment service providers, participants of the European and international payment systems and their related parties, insurance service providers and financial service agents, third parties involved in the execution of transactions;

6.2.3. Other VIALET customers that details are stored in Customer's phone contact list in case if the Customer accepted VIALET access to Customer's contact list in Customer's mobile phone settings. By accepting contact list sharing with VIALET, the Customer:

- became visible to other VIALET customers who saved him/her as a contact in their phone book;
- allows VIALET to disclose to other customers that the Customer has an account with VIALET and, in case of payment order, - Customer's account number;
- allows VIALET to provide such service as receive and send payments directly to Customer phone contacts without entering their account numbers;

6.2.4. State institutions, authorities and other statutory persons based on written requests or the duties binding upon VIALET stipulated by the legal acts;

6.2.5. Providers of databases and registers, e.g. to credit registers, population registers, commercial registers, securities registers, pension register, controllers who process consolidated debtor files, or other register holding or intermediating Personal data, debt collectors, bailiffs, notaries or insolvency administrators;

6.2.6. VIALET audit firms, financial and legal service providers, translators or any other service providers of VIALET.

7. Advertising and direct marketing

7.1. VIALET's advertising and direct marketing communications (e.g. about VIALET's services and related campaigns) are sent to Customers who have consented to receiving direct marketing and commercial communications from VIALET. Such Customers receive VIALET commercial communications and direct marketing communications via their preferred means of communication.

7.2. The Customer may give his/her consent to the receipt of commercial communications of VIALET by visiting https://vialet.eu/, registering on the website https://ib.vialet.eu or https://hub.vialet.eu/ or mobile application, as well as by providing application forms.

7.3. A customer's consent to receive commercial communications is valid until its withdrawal. Customers have the right to object to the processing of their Personal data for direct marketing purposes at any time and free of charge. To exercise this right, the Customer should contact VIALET or opt out of receiving the advertising and commercial communications using the link provided in the e-mail message or following other instructions as provided in such direct marketing communication.

8. Profiling, personalized offering and automated decision making

8.1. Profiling refers to the automatic Processing of Personal data used to assess certain personal characteristics of a Customer, for example, the economic situation, personal preferences, interests, place of residence of such an individual. Profiling is, for example, used to make analysis for Customer advice, marketing purposes, system development, for automated decision-making such as credit assessments, for risk management and for transaction monitoring to counter fraud.

8.2. VIALET may make automated decisions for identity check, risk management, anti-money laundering and international sanctions checks, politically exposed persons check, for monitoring the Customer's account and Customer behavior in using VIALET products to detect fraud and financial crime and implement international sanctions. In these cases, manual decision making could be also involved.

8.3. Depending on the product, VIALET may use automated decisions in calculating the credit limit or interest rate that VIALET could offer the Customer. VIALET automatically analyzes information relating to the Customer, such as loan history, habits that VIALET has identified in connection with the use of its services or information that VIALET is authorized to obtain from third parties.

8.4. VIALET may also collect statistical data regarding the Customer, such as typical behavior and lifestyle patterns based on demographic household data. Statistical data for creating segments profiles can be collected from external sources and may be combined with VIALET internal data.

8.5. If VIALET makes an automated decision about the Customer that significantly affects him, the Customer can ask VIALET to carry out a manual review of this decision.

9. Geographical area of processing

9.1. As a general rule the Personal data are processed within the European Union/European Economic Area (EU/EEA).

9.2. Given the global nature of financial services and technological solutions and to process Personal data for the purposes specified in the Policy, for the provision of individual services Personal data may be transferred for Processing to the Personal data receivers located outside the European Union and the European Economic Area, for instance, if their services are provided by a counterparty (processor, separate controller, joint controller). Any such international transfer of Personal data is done in compliance with the requirements of the applicable laws. The transfer and processing of Customer data outside of the EU/EEA can take place provided there is a legal basis and appropriate safeguards are in place. Appropriate safeguards include for example:

- The EU Standard Contractual Clauses or other approved clauses, code of conducts, certifications approved in accordance with the GDPR.

- The country outside of the EU/EEA where the recipient is located has an adequate level of data protection as decided by the EU Commission.

10. Retention period

10.1. The period for which VIALET stores Personal data depends on the purposes for which VIALET processes it and under which criteria it assesses Personal data storage periods.

10.2. When determining Personal data storage periods, VIALET assesses:

10.2.1. the need to store Personal data to ensure performance of a valid service agreement;

10.2.2. the need to store Personal data for VIALET to fulfill its legal obligations, for instance, within the 8-year period stipulated in the AML/CTF Law and within the different storage periods specified in other legal acts;

10.2.3. storage of Personal data to safeguard VIALET interests in different claims in case of termination of business relationships with Customer, for instance, 10 years in accordance with the general limitation period for liability.

10.2.4. VIALET legitimate interests or those of a third party that might be offended in the event of erasure of Personal data, for instance, with respect to Customer right to restrict data processing;

10.2.5. the need to store Personal data in order to provide proof of the legitimate Processing of Personal data in the previous period, for instance, Customer Consent to the previous Processing operations;

10.2.6. if Personal data processing is performed based on the Consent, until the Consent for the respective Personal data Processing purpose is in force given that there is no other basis for the Processing of Customer's Personal data.

10.3. In assessing the Personal data storage periods, VIALET takes into account the purpose of Persona data processing. If VIALET identifies different reasonable periods for storing Personal data, for instance, between the statutory storage period and the timeframe for protecting VIALET interests, this will be a reasonable basis to store Personal data for a longer period.

10.4. If one or more of the specified criteria occur, VIALET will ensure that Customer Personal data is deleted or anonymized.

11. Customer's rights as a data subject

11.1. A Customer (data subject) has rights regarding his/her data Processing that is classified as Personal data under applicable law. Such rights are in general the following:

11.1.1. Require his/her Personal data to be corrected if it is inadequate, incomplete or incorrect;

11.1.2. Object to Processing of his/her Personal data, if the use of Personal data is based on a legitimate interest, including profiling for direct marketing purposes (such as receiving marketing offers or participating in surveys);

11.1.3. Require the erasure of his/her Personal data, for example, that is being processed based on the consent, if he/she has withdrawn the consent. Such right does not apply if Personal data requested to be erased is being processed also based on other legal grounds such as agreement or obligations based on applicable law;

11.1.4. Restrict the Processing of his/her Personal data under applicable law, e.g. during the time when VIALET assesses whether the Customer is entitled to have his/her data erased;

11.1.5. Receive information if his/her Personal data is being processed by VIALET and if so then to access it;

11.1.6. Receive his/her Personal data that is provided by him/herself and where feasible transmit such data to another service provider (data portability);

11.1.7. Withdraw his/her consent to process his/her Personal data;

11.1.8. Not to be subject to fully automated decision - making, including profiling, if such decision - making has legal effects or similarly significantly affects the Customer. This right does not apply if the decision - making is necessary in order to enter into or to perform an agreement with the Customer,

if the decision - making is permitted under applicable law or if the Customer has provided his/her explicit consent;

11.1.9. Lodge complaints pertaining to the use of Personal data with the State Data Protection Inspectorate, website address: https://vdai.lrv.lt/, the registered address at L. Sapiegos str. 17, Vilnius, the Republic of Lithuania, phone No.: +370 5 271 2804, fax. +370 5 261 9494, email: ada@ada.lt, if he/she considers that Processing of his/her Personal data infringes his/her rights and interests under applicable law.

11.2. VIALET makes every effort for the implementation of Customer's rights and for answering all questions that arise to the Customer regarding the present Policy and matters envisaged in it. Customers may lodge a request regarding the exercise of the above-indicated rights as well as any complaints, notices or requests (hereinafter the 'Request') to the Data Protection Officer.

11.3. To prevent money laundering, as a financial institution VIALET must process Personal data about customers and persons, with whom business relations have not been started or have been terminated in compliance with the procedure specified in the Law on the Prevention of Money Laundering and Terrorist Financing and Law on the Implementation of Economic and other International Sanctions of the Republic of Lithuania. Processing of Personal data can include information about these persons' beneficial owners and authorized persons. In these cases, the Personal data Processing is not subject to the Data subjects' rights specified in the General Data Protection Regulation to claim information about data Processing, including its purposes, recipients, and sources. Under the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania, Data subjects are not entitled to access their data and request to rectify, object, require the erasure, stop or restrict data processing. Although, Data subject has the right to request that a supervisory authority confirms the lawfulness of the Processing.

11.4. VIALET will reply to Customer Request within a period of not more than 30 (thirty) calendar days since the day of receipt of the Request unless a different period is specified in the applicable legislation.

11.5. VIALET will usually not charge the Customer a fee when he/she exercises his/her rights. However, VIALET is allowed by law to charge a reasonable fee or refuse to act on the Customer's request if it is manifestly unfounded or excessive.

12. Contact details

12.1. Customers may contact VIALET with any enquiries, withdrawal of consents, requests to exercise data subject rights and complaints regarding the use of Personal data.

12.2. Contact details of VIALET are available on VIALET website vialet.eu.

12.3. Contact details of the appointed Data Protection Officer - e-mail: dataprotection@vialet.eu, at the postal address: Via Payments UAB, Konstitucijos pr. 7, Vilnius, LT-09308 with a notice "Data Protection Officer".

13. Validity and amendments of the privacy policy

13.1. VIALET is entitled to amend the Policy at any time unilaterally, in compliance with the applicable law, by notifying the Customer of any amendments via the website of VIALET.