Last updated: 30/12/2025

Privacy Policy

General definitions

1. Personal data means any information relating to an identified or identifiable natural person (Data Subject), as specified in Article 4(1) of the GDPR.
2. GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
3. Data processing means any operation or set of operations which is performed on personal data or on sets of personal data, as specified in Article 4(2) of the GDPR.
4. Data Processor means a natural person or legal entity which processes personal data on behalf of the Data Controller, as specified in Article 4(8) of the GDPR.
5. Data Controller, the entity determining the purposes and means of processing personal data, is Paysera LT, UAB, managing the payment initiation and account information service, peer-to-peer lending platform, qualified e-identification, and other services. According to the Joint Controller Agreement No. 2018019 of 19/09/2018, your personal data Controller is the Paysera network (hereinafter referred to as Paysera, Operator, Data Controller, or Company). Contact details of Paysera are published on the Paysera website. The contact details of the Data Protection Officer appointed by Paysera are: dpo@paysera.com.
6. **Joint Data Control** – Paysera LT, UAB, together with other network companies and the coordinator Paysera Tech (Cayman Islands), acts as Joint Controllers in accordance with Annexe No. 16 "Network Data Governance Agreement" to the Joint Action Agreement. This agreement regulates the allocation of responsibilities and ensures data protection within the network. Personal data is processed jointly solely to ensure network security and operational integrity, specifically: for the prevention of money laundering and terrorist financing; for fraud detection; for the management of security incidents; and for ensuring uninterrupted client support when services are provided by another network partner.
7. **Data Subject or Client** – a natural person who intends to enter into, or has entered into, a business relationship with the Data Controller (e.g., profile creation, opening a payment account, obtaining a qualified electronic identification means, submitting a consumer credit application, acting as a consumer credit lender or funder, concluding a service provision agreement with the Company, etc.), or whose business relationship has ended but whose data is still processed by the Data Controller in accordance with legal provisions.
8. **Platform** – a software solution hosted on websites belonging to the Company, developed by the Company and used to provide the Company's services.

General provisions

9. Personal data collected by Paysera is processed in accordance with the Law on Legal Protection of Personal Data of the Republic of Lithuania, the GDPR, and other legal acts. All persons, representatives, and employees of representatives acting on behalf of Paysera who have the ability to access systems with Client data, access them exclusively for the performance of their work functions, having a legitimate basis for such access, and must keep personal data known during work confidential even after the termination of employment or contractual relationships.
10. The Company, in accordance with the applicable legal requirements, shall ensure the confidentiality of personal data and the implementation of appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure, accidental loss, alteration, destruction, or other unlawful processing.
11. This Privacy Policy sets out the basic rules for the collection, storage, processing, and retention of your personal data, other information relating to you, the scope, purpose, sources, recipients, and other important aspects of your personal data processing when you use Paysera as a payment service provider. In this Privacy Policy, terms used in the singular form also include the plural form, and terms used in the plural form also include the singular form, unless the context clearly indicates otherwise.
12. By accessing the Paysera website and/or using the app, and/or the information contained therein, and/or services, you acknowledge and confirm that you have read, understood, and agree to this Privacy Policy. Also, after you register with the system and start using Paysera services, this Privacy Policy becomes a Supplement to the General Payment Services Agreement.
13. Paysera reserves the right, at its sole discretion, to modify this Privacy Policy at any time by publishing an updated version of the Privacy Policy on the website and, if the changes are substantial, notifying registered users by email or in-app notification. An amended or updated version of this Privacy Policy shall take effect upon its publishing on the website.
14. If the user of the services is a business client, this Privacy Policy applies to individual clients whose data is transmitted to Paysera by the business client. The user shall inform the Data Subjects (managers, recipients, agents, etc.) of the transfer of their data to Paysera in accordance with Article 14 of the GDPR.

Data processing purposes, providers, deadlines, recipients

15. The main purpose for which Paysera collects your personal data is to provide the payment services of Paysera to clients who send and receive payments. As a provider of payment, qualified e-identification, peer-to-peer lending, self-service terminals, and POS services, Paysera is bound by law to establish and verify your identity prior to entering into financial services transactions with you, also, at the time of the provision of the services, to request further information, as well as assess and store this information for the retention period set out by legislation. Taking this into account, you must provide correct and complete information.

PURPOSE: Client identification, provision of payment (account opening, transfers of funds, payment processing, and other), ATMs, self-service terminals, qualified e-identification services, prevention of money laundering and terrorist financing, submission of reports to state authorities, implementation of other legal obligations of the payment service provider.

16. Personal data is processed for this purpose in compliance with legal requirements related to: establishment and verification of the client's identity; conclusion and execution of agreements with the Client or in order to take steps at the request of the client; execution of transfers of funds and transmission of the necessary information together with a transfer in accordance with legislation; implementation of the "Know Your Client" requirements; continuous and periodic monitoring of the client's activity; risk assessment; updating Client data in order to ensure its accuracy; prevention of possible money laundering and terrorist financing, prevention of fraud, detection, investigation and

informing of such activity, determination of politically exposed persons or financial sanctions imposed on the client; ensuring proper risk and organisation management.

17. For this purpose, the following personal data may be processed: name, surname, gender, national identification number, date of birth, a face photo, direct video transmission (direct video broadcast) recording, citizenship, country of birth, country of residence, data from an identity document (including but not limited to a copy of the document), address, email address, phone number, current payment account number, IP address, current professional or work activity, current public function, data on the client's participation in political activities, inclusion in sanctions lists, other data required by applicable anti-money laundering and counter-terrorist financing laws, as well as Client location data, planned service, account usage purpose (personal/business), planned investment amount, income received, main source of funds, origin of funds, beneficial owner, information about the ultimate beneficiary: first name, last name, nationality, personal identification number (national ID number), date of birth, address, basis of authorisation, political involvement, other data specified in the client's "Know Your Client" (KYC) questionnaire, business relationship correspondence with the client, documents and data confirming the monetary operation or transaction, or other legally valid documents and data related to the execution of monetary operations or transactions, tax residence country, connection with the EEA/EU, tax identification number, devices used, data related to the user's mobile device, model, operating system, whether the device is rooted, whether the device is an emulator, IP address, Wi-Fi SSID, Wi-Fi MAC, device system language, SIM card issuing country, SIM card operator, device pseudo-unique ID, Android ID, Android GSFID, Android fingerprint, web-view version, Paysera app version, history of monetary transactions.
18. This personal data is collected and processed in the performance of the public authority functions assigned to the Data Controller, and on the basis of a legal obligation imposed on the payment service provider, i.e. the Law on Payments, the Law on Electronic Money and Electronic Money Institutions, laws on the prevention of money laundering and terrorist financing, and other applicable legal acts, and is required in order to open an account and/or provide a payment service.
19. Data retention period: 10 (ten) years after the termination of the business relationship with the client. This personal data must be retained for 8 (eight) years according to the Law on Prevention of Money Laundering and Terrorist Financing. This data is retained for another 2 (two) years on the basis of the legal interests of Paysera according to the ordinary limitation period of the lawsuit.
20. Data providers and sources:
    20.1.The data subject directly;

    20.2.Third parties:

    20.2.1.Credit and other financial institutions and their branches;

    20.2.2.State and non-state registers;

    20.2.3.Databases for checking the data of identity documents (databases of expired documents and other international databases);

    20.2.4.Authority check registers (registers of notarised authority and other databases);

    20.2.5.The Register of Incapacitated and Disabled Persons;

    20.2.6.The Population Register, other databases;

    20.2.7.Companies processing consolidated debtor files (e.g. in Lithuania, UAB "Creditinfo Lithuania", UAB "Scorify", or other);

    20.2.8.Companies maintaining registers of international sanctions;

    20.2.9.Law enforcement agencies;

20.2.10.Bailiffs;

20.2.11.Legal entities (provided you are a representative, employee, founder, shareholder, participant, contractor, or the real beneficiary of these legal entities);

20.2.12.Partners or other legal entities that engage us or are engaged by us in the provision of services;

20.2.13.Social networks where you have a profile linked to our system;

20.2.14.Other persons.

21. In order to more effectively fulfil our legal obligations – for example, to identify potentially suspicious financial transactions for the purpose of preventing money laundering or to verify the authenticity of identity documents – we may use artificial intelligence (AI) solutions (tools may be trained using existing data or data may be analysed by the tools). These tools assist in processing large volumes of data and identifying discrepancies; however, any final decisions that may have significant consequences for you are always reviewed and approved by our employees.
22. Groups of data recipients: supervisory authorities, credit, financial, payment and/or electronic money institutions, pre-trial investigation institutions, state tax agencies, payment service representatives or partners of Paysera (if the transaction is carried out using their services), recipients of transaction funds receiving the information in payment statements together with the funds of the transaction, the recipient's payment service providers and correspondents, participants, and/or parties related to national, European, and international payment systems, debt collection and recovery agencies, companies processing consolidated debtor files, lawyers, bailiffs, auditors, other entities having a legitimate interest, other persons under an agreement with Paysera or on other lawful bases.

PURPOSE: Dispute and debt management.

23. Personal data under this purpose is processed in order to resolve disputes, manage and collect debts, submit claims, demands, lawsuits, etc.
24. For this purpose, the following personal data may be processed: name, surname, national identification number, address, date of birth, data from an identity document, email address, phone number, current account number, IP address, current account statements, video and audio recordings, and all other data related to the circumstances in which the dispute or debt arose.
25. Data retention period: the due date for the debt is 10 (ten years) from the day the debt became known (if the debt consists of several elements – from the date the last element became known), and after the opening of legal proceedings – 10 (ten years), but not shorter than until the complete fulfilment of the parties' obligations to each other. The data retention period is based on the limitation periods for proceedings set out by the Civil Code of the Republic of Lithuania.
26. Data providers: the Data Subject directly, credit, financial, payment and/or electronic money institutions, state and non-state registers, companies processing consolidated debtor files (e.g. in Lithuania, UAB "Creditinfo Lithuania" or other), providers of electronic communications services, other persons.
27. Groups of data recipients: companies processing consolidated debtor files, credit, financial, payment and/or electronic money institutions, lawyers, bailiffs, courts, pre-trial investigation institutions, state tax agencies, debt collection and recovery agencies, and other entities having a legitimate interest.
28. Please note that if you have a debt to Paysera and you are postponing the performance of your identity, contact details, and credit history, i.e. financial and property liabilities and information on their execution, and debts and their payment to companies managing debtors' databases (such as the credit institution UAB "Creditinfo Lithuania" in Lithuania*), as well as to debt collection companies. You can access your credit history by contacting the credit bureau directly.

PURPOSE: To provide business clients using the Paysera POS service with the technical capability to manage their customers' and purchase data, ensuring the functionality of payment processing, invoicing, and other processes related to the Paysera POS service, while fully complying with the GDPR and all other applicable legal requirements.

29. For this purpose, the following data are collected and processed: data of the Paysera POS Client and the natural persons representing them (first name, surname, relationship with the Paysera POS Client (position/role, etc.), personal/tax payer's identification number, contact details such as address, telephone number and email address), payment transaction information (card type, last four digits of the card number, transaction number), as well as purchase data (order items, quantity, price, discounts, purchase date, order number and fiscal data). Data retention period: 10 (ten) years after the termination of the business relationship with the client. This personal data must be retained for 8 (eight) years according to the Law on Prevention of Money Laundering and Terrorist Financing. This data is retained for another 2 (two) years on the basis of the legal interests of Paysera according to the ordinary limitation period of the lawsuit.
30. **With regard to the data uploaded into the system by the Paysera POS client**, Paysera acts as the Data Processor, while the Paysera POS Client is the Data Controller. The Paysera POS Client confirms and undertakes to process this data in accordance with the requirements of Article 6 of the GDPR. The retention period for this data is determined by the internal operational documents of the Data Controller (the Paysera POS client), taking into account the legal requirements for retaining accounting documents and other applicable deadlines. Paysera, in providing the technical infrastructure, retains backup copies only for as long as necessary to ensure the functioning of the service or as required by law. Upon termination of the agreement with the Paysera POS client, Paysera has the right to delete all personal data stored in the client's Paysera POS account after 90 (ninety) days, unless legislation requires them to be retained for a longer period. This period is intended to ensure the smooth transfer of data or final settlements. Data in the Paysera POS system backups may be retained for a longer period; however, they are isolated and not processed within active systems, until they are ultimately deleted in accordance with the established backup rotation cycle.
31. Data sources (where we obtain the data from): The primary source is the Client, who enters information about themselves, their customers, and purchase transactions into the Paysera POS system. Partial payment data may also be received from service providers processing payment card transactions (e.g., card type, the last four digits of the card number, transaction number).
32. Data recipients: The business client, as the Data Controller, has access to the data they have entered. Paysera and its authorised service providers (e.g., IT infrastructure or data centre service providers) process this data only to the extent necessary to provide and improve the service or as required by law. Information is provided to state authorities only in cases prescribed by legislation.

PURPOSE: To collect payments through Paysera self-service terminals and to provide reports to clients, in order to ensure an efficient and secure payment process and the delivery of necessary information.

33. For this purpose, depending on the payment collection location, the following data may be collected: first name, surname, date of birth, personal identification number, email address, patient code issued by a healthcare institution, student study programme and year of study, payment card type, the last four digits of the card number, transaction number, as well as any other data provided by the individual when making a payment.
34. The data are collected and processed on the basis of contract performance (Article 6(1)(b) of the GDPR) or legal obligations set out in legislation (Article 6(1)(c) of the GDPR), and Paysera acts as the Data Processor by enabling the entry and storage of the data and ensuring the technical functionality of the service.
35. Data retention period: this is determined by the Data Controller, who must comply with legal

requirements regarding the retention of accounting and other records. Paysera stores only the data termination of the business relationship, Paysera retains self-service terminal data for no longer than 3 (three) years after the end of the relationship.

36. Data providers: the primary providers are the individuals themselves, who submit the required data when using Paysera self-service terminals. Based on this data, individuals are identified in the databases of the entity collecting the payments (the organisation for whom the specific terminal is used to collect payments). Partial information about card transactions is also received from payment processing service providers.
37. Data recipients: depending on the information required for payment collection, this data may be transferred to the specific Paysera Client collecting payments via the terminals – such as a healthcare institution, car dealership, educational institution, or another business or public entity that uses a particular Paysera self-service terminal and has a lawful basis to receive payment transaction information. Data may also be provided to the relevant state authorities where required by law or where necessary to protect legitimate interests.

PURPOSE: To support and administer relations with clients, inform clients about existing and new services, provide services, prevent disputes, and collect evidence (recording phone conversations), correspondence of business relations with the Client.

38. Personal data is processed for this purpose in order to: maintain the business relationship and communication with the Client; provide services to the client; protect the interests of the Client and/or Paysera; prevent disputes, provide evidence of business communication with the Client (recordings of conversations, correspondence); perform quality assessment and ensure the quality of services provided by Paysera; where it is necessary for the execution of the agreement, in order to take steps at the request of the Client, or in implementing a legal obligation; inform the Client about the services provided by Paysera, their prices, specifics, changes in the contracts concluded with the Client, etc.; send Paysera systemic and other notifications related to the services provided.
39. For this purpose, the following personal data may be processed: name, surname, address, date of birth, email address, phone number, IP address, Client location data, current account statements, phone conversation recordings, correspondence with the Client, and any other data necessary for the purpose.
40. Data retention period: no longer than 10 (ten) years from the date of the conversation, taking into account the ordinary limitation period of the lawsuit. Paysera reserves the right to delete such data at any time. Such data retention period is required under the laws on the prevention of money laundering and terrorist financing.
41. Data providers: the data subject directly, providers of electronic communications services.
42. Data recipients: supervisory authorities, companies processing consolidated debtor files, lawyers, bailiffs, courts, pre-trial investigation institutions, debt collection and recovery agencies, other entities having a legitimate interest, other entities under an agreement with Paysera.
43. The Data Subject confirms that they understand that such information notifications are necessary for the performance of the General Payment Services Agreement and/or its annexes concluded with the Client, and do not constitute direct marketing messages.

PURPOSE: To ensure the identification of the Paysera user and the secure, lawful and proper execution of the transaction initiated by them at the ATM.

44. For this purpose, the following data are collected: a temporarily generated scannable code that is linked to the Paysera app and has a limited validity period; the type of transaction (cash-in/cash-out); the date and time; the cash-in/cash-out amount; ATM identification information (unique ATM number, address or other location markers); the user's unique number (linked to the Paysera account); and a callback confirmation indicating that the user has been successfully authenticated. Additionally, video surveillance material (photos and video recordings) is collected.

45. The data are collected and processed on the basis of contract performance (Article 6(1)(b) GDPR) between the ATM service provider and the user, as well as on the basis of a legal obligation (Article 6(1)(c) GDPR) to comply with requirements under payment, electronic money, anti-money laundering, and other applicable legislation, and on the basis of a legitimate interest (Article 6(1)(f) GDPR) to ensure payment security and prevent fraud.
46. Data retention period: the generated scannable code is valid only for a short period (up to 5 minutes), and the generated Client identification number is valid only for the duration of the transaction. Key transaction data (date, location, cash-in/cash-out amount, etc.) are stored in the ATM for 2 years. The ATM operator retains this data for 5 (five) years from the date of the transaction. Video surveillance recordings are retained for up to 5 (five) months, unless there is a need to store them for a longer period, for example, in the course of a law enforcement investigation or dispute (in which case the material may be retained until the need ends).
47. The Client is identified using a scannable code generated by the Paysera app, which the user presents to the ATM. Additional Client data may be obtained from a video surveillance camera, if installed.
48. Data recipients: video recordings or other data may, when necessary, be provided to law enforcement authorities during investigations, or to other state authorities if required by law.

PURPOSE: Creditworthiness assessment, credit risk management, and automated decision-making.

49. The personal data for this purpose is processed to assess the creditworthiness of clients, to manage the credit risk, and to meet the requirements related to operational risk management and capital adequacy, so that Paysera can offer/provide funding.
50. The following personal data may be processed for this purpose: name, surname, address, date of birth, email address, telephone number, payment account number, IP address, payment account statements, Client's balance on the account, financial liabilities, credit and payment history, income, education, workplace, current work position, work experience, available assets, and data on relatives, credit rating, former debts, and other information.
51. Data retention period: 1 (one) year after the termination of the business relationship with the Client, when the end date is not earlier than the date of full fulfilment of obligations by both parties to each other. In the event of a refusal to grant credit, the moment of informing the Client about the refusal to grant credit shall be considered the moment of termination of the relationship with the Client.
52. Data providers: the Data Subject directly, credit and other financial institutions and their branches, law enforcement agencies, other registers and state institutions, companies processing consolidated debtor files (e.g. in Lithuania, UAB "Creditinfo Lithuania", UAB "Okredo"), individual persons who provide data about spouses, children, and other persons related by kinship or affinity, co-debtors, guarantors, collateral providers, etc., legal entities when the Client is a representative, employee, contractor, shareholder, participant, owner, etc. of these legal entities, and partners or other legal entities engaged by Paysera to provide services to you.
53. Data recipients: credit, financial, payment and/or electronic money institutions or service providers assisting in the assessment of creditworthiness, and companies processing consolidated debtor files.
54. In order to conclude or offer to enter into a funding agreement with you and to provide you with services, Paysera will, in certain cases, apply decision-making based on the automated processing of your personal data. In this case, the system checks your creditworthiness with a set algorithm and assesses whether the service can be provided. If the automated decision is negative, it may be changed by the Client providing more data. Paysera takes all the necessary measures to protect your rights, freedoms, and legitimate interests. You have the right to demand human intervention, express your opinion, and challenge an automated decision. You have the right to oppose an automated decision by contacting Paysera directly.

PURPOSE: Provision of services through third parties.

55. Personal data for this purpose is processed in order to ensure the widest possible range of services received by Paysera clients, with certain services being provided by third parties.
56. For this purpose, the following personal data may be processed: name, surname, citizenship, personal identification number, address, contact information.
57. The Client is clearly informed about any data processing for the purpose of providing services through third parties, and the data is processed only with the Client's expressed consent.
58. Data retention period: 1 (one) year.
59. Data providers: the data subject directly, Paysera, third parties providing services.
60. Data recipients: third parties providing services, Paysera, Data Subject.

PURPOSE: Protection and safeguarding of the interests of Paysera and the Client (video surveillance monitoring on Paysera premises and audio recording in the client service centre).

61. Personal data are processed for this purpose on the basis of legitimate interests under Article 6(1)(f) of the GDPR. These interests include ensuring security (protecting the health, life, and property of employees, Clients, and other visitors from unlawful acts such as theft, vandalism, or physical assaults), protecting rights and legitimate interests (collecting objective evidence for investigating incidents, accidents, or disputed situations), and ensuring the accuracy and transparency of services. Audio recordings help accurately capture your verbal request regarding a financial transaction and ensure it is executed correctly, thereby preventing errors that could cause losses to you or the Company. They also assist in objectively resolving disputes regarding the content, amount, or other terms of a transaction, and in ensuring compliance with legal requirements. Audio and video recordings help us verify and demonstrate that employees have properly followed anti-money laundering and counter-terrorist financing procedures, including KYC requirements, mandatory questioning, and recording of responses during identification, as well as assisting in the investigation of incidents and errors (helping to determine the causes if an incident occurs, an operational error takes place, or a cash discrepancy is identified).
62. For this purpose, the following personal data may be processed: video recordings on the premises managed by Paysera, video and audio recording data in the client service centre.
63. Video surveillance and recording is conducted in a large part of Paysera premises, including common areas accessible to all visitors, the client service area, and rooms with restricted access (e.g., office spaces, kitchens), in order to ensure internal order and the security of property. Audio recording is conducted only in the client service centre, at the service counter, where financial transactions and Client identification take place. Sound is not recorded in other areas of the premises. Before entering the premises of Paysera where video surveillance is conducted, you are informed about the surveillance by special markings.
64. Video and audio recordings are retained for up to 1 (one) year from the date of recording. This retention period is necessary to ensure the ability to detect and investigate incidents within a reasonable timeframe, resolve potential disputes (which may extend up to one year or longer), and comply with law enforcement requests for data. After this period, the data are deleted, unless they are required for an ongoing investigation, dispute resolution, or other cases prescribed by law – in which case they are retained for as long as necessary to achieve these purposes.
65. Data providers: the data subject directly who visits the premises of Paysera where video surveillance is conducted and is captured by the surveillance camera.
66. Data recipients: video and audio recordings are treated as confidential. Access to them is strictly limited and granted only to employees who require it to perform their job functions ("need-to-know" principle), and solely for the purposes described above. Recordings may also be provided to courts, pre-trial investigation authorities, and lawyers. Internal review of recordings is conducted only when there is a clear need – for example, when investigating an incident, resolving a dispute, checking cash discrepancies, or carrying out periodic, randomly selected audits (very limited in scope, e.g., a few recordings of clients served by an employee per month) – to ensure compliance with anti-money

laundering, KYC, and other essential procedures, as well as to monitor service quality.

PURPOSE: Direct marketing.

67. For this purpose, personal data is processed in order to provide clients with offers on the services provided by Paysera and find out the clients' opinions on the above-mentioned services.
68. The following personal data may be processed for this purpose: name, surname, email address, and phone number.
69. For this purpose, Paysera sends newsletters and direct marketing messages after obtaining the Client's consent. Paysera may use a newsletter service provider while ensuring that said provider complies with the personal data protection requirements set out in the Joint Controller Agreement. The Client may revoke their consent upon receiving newsletters or direct marketing messages by clicking on the Revoke your consent link as well as informing Paysera at any time about their refusal to process personal data for direct marketing purposes by e-mail support@paysera.com.
70. Data retention period: until the termination of the business relationship with the Client or until the day the Client objects to the data processing for this purpose.
71. Data providers: the Data Subject directly.
72. Data recipients: The data for this purpose may be transmitted to search or social networking systems (the possibility to object data processing is ensured by the websites of these systems), newsletter service providers.

PURPOSE: Statistical analysis, service improvement.

73. Your personal data collected and anonymised for the aforementioned purposes may be processed according to Article 6.1(f) of the GDPR for the purpose of statistical analysis and for improving technical and organisational measures, information technology infrastructure, ensuring the adaptation of the provided service to the devices used, creating new Paysera services, increasing satisfaction with existing services, testing and improving technical measures and IT infrastructure. For this purpose, personal data shall be processed in such a way that, by including it in the scope of statistical analysis, it is not possible to identify the Data Subjects concerned. The collection of your personal data for the purpose of statistical analysis is based on the legitimate interest to analyse, improve, and develop the conducted activity.
74. You have the right to disagree and object to your personal data processing for such purpose at any time and in any form by informing Paysera thereof. However, Paysera may continue to process the data for statistical purposes if it proves that the data is processed for compelling legitimate reasons beyond the interests, rights, and freedoms of the Data Subject or for the establishment, exercise, or defence of legal claims.

PURPOSE: Prevention of service misuse and criminal offences, and ensuring proper delivery of services.

75. The data collected for all of the above purposes may be used to prevent unauthorised access and use, i.e. to ensure privacy and information security.
76. For the processing of personal data, Paysera may engage Data Processors and/or, at its own discretion, hire other persons to perform certain ancillary functions on behalf of Paysera (e.g. data centres, hosting, cloud hosting, system administration, system development, software development, provision, support services such as improvement and development; services of client service centres; marketing, communication, consulting, temporary staffing, or similar services). In such cases, Paysera shall take the necessary measures to ensure that such Data Processors process personal data in accordance with Paysera's instructions and applicable laws, and shall require compliance with the appropriate personal

data security measures. Paysera shall also ensure that such persons are bound by confidentiality obligations and cannot use such information for any purpose other than the performance of their functions.

77. Personal data collected for the purposes specified in this Privacy Policy shall not be processed in any ways incompatible with these legitimate purposes or legal requirements.
78. The data referred to above will be provided and received through a software tool used by Paysera or its authorised agent, also by other means and third persons with whom Paysera has entered into personal data processing agreements in accordance with laws and regulations.

Geographical area of processing

79. Generally, personal data is processed within the European Union/European Economic Area (EU/EEA). However, in order to provide you with services, ensure the continuity of our network operations, and engage specialised partners worldwide, your data may, in certain cases, be transferred to and processed outside the EU/EEA (hereinafter referred to as "Third Countries"). Data transfers to Third Countries that do not benefit from an European Commission adequacy decision are carried out in accordance with the Network Data Governance Agreement. This agreement ensures the automatic application of the Standard Contractual Clauses (SCCs) approved by the European Commission to all data transfers between network members, guaranteeing that your data is protected in compliance with GDPR requirements, regardless of the partner's location.
80. Your personal data may be transferred to the following categories of recipients in Third Countries:
    80.1.For infrastructure and platform partners. Our services are provided using the shared Paysera network IT infrastructure, which is managed and maintained by our strategic partner. Although this partner operates through a holding company registered in the European Union, its primary place of registration is the Cayman Islands. Please note that technical access and administrative data necessary to ensure the platform's operation, security, and maintenance are not accessible from this jurisdiction, and all data is stored within the EU / EEA territory. Data transfers to Third Countries that do not have a European Commission adequacy decision are carried out in accordance with a Joint Activity Agreement, which provides for the automatic application of the European Commission–approved Standard Contractual Clauses (SCCs) to all data transfers between network partners. This ensures that your data is protecte in accordance with GDPR requirements, regardless of the partner's location.

    80.2.Paysera network partners. We operate as part of an international corporate network. When you use services involving our partners, or your transactions are related to them, your data may be transferred to these partners, which operate in Third Countries such as the Republic of Albania, the Republic of Kosovo, Georgia, and others.

    80.3.External service providers and specialists. To ensure uninterrupted, 24/7, high-quality Client support, compliance with KYC procedures, and other functions, we engage trusted partners and specialists operating in Third Countries such as Morocco, the Philippines, India, and others. These service providers are granted secure access to your data solely for the purpose of performing the functions assigned to them (e.g., verifying documents you have submitted or responding to your inquiries).

    80.4.International payments initiated by you. When you personally initiate a payment transfer to a recipient located in a Third Country, we are required to transmit your personal and payment data to the financial institution (correspondent bank) in that country in order to execute your instruction.

81. As the aforementioned Third Countries are not required to apply EU-level data protection, one or more of the following GDPR-prescribed safeguards are applied to each data transfer:

81.1.Standard Contractual Clauses (SCCs). For all system-related data transfers within the Paysera infrastructure, we have entered into Standard Contractual Clauses (SCCs) with the data recipients for the transfer of personal data to Third Countries, as approved by the European Commission. These agreements legally oblige the data recipients to process your data in accordance with EU data protection standards.

81.2.Additional technical and organisational measures are implemented, for example: end-to-end encryption, pseudonymisation where possible to reduce the amount of directly identifiable information, strict access controls to ensure that only those who need access can reach the data, and contractual obligations for the data recipient to promptly inform us of any requests from authorities to disclose data and to legally challenge such requests where possible.

82. For international payments initiated by you (point 80.4), the transfer of data is based on the exception under Article 49 of the GDPR, as the transfer is necessary for the performance of the agreement between you and us (i.e., to carry out the payment transfer you have instructed).

Profiling and automated decision-making

83. To provide you with fast, secure, and modern services and to fulfil our legal obligations, we use advanced technologies, including automated systems and artificial intelligence (AI) solutions. These technologies help us process your personal data automatically to assess certain personal characteristics (profiling) and, in some cases, to make decisions without direct human intervention (automated decision-making).
84. Profiling and automated decision-making for the purpose of creditworthiness assessment and credit risk management:
84.1.When entering into, or intending to enter into, a consumer credit or other financing agreement with you, we are legally obliged to responsibly assess your creditworthiness and manage the associated risk. For this purpose, we may engage third parties (e.g., UAB "Scorify") to use an automated decision-making system.

84.2.The system, based on algorithms and AI models, may automatically collect and analyse your personal data (detailed information about the data categories and sources can be found in the section of this Privacy Policy titled *Creditworthiness assessment, credit risk management, and automated decision-making* (points 49–54)). The system evaluates a variety of factors, such as:

84.2.1.The ratio of your income to your financial obligations;

84.2.2.The reliability of your credit history (payment discipline, presence of overdue debts);

84.2.3.Other factors directly related to your ability to meet your financial obligations.

84.3.Based on this analysis, the system automatically makes one of the following decisions, which may create legal and financial obligations for you:

84.3.1.Approve your application and offer financing;

84.3.2.Offer you alternative financing terms (e.g., a lower amount or different repayment schedule);

84.3.3.Reject your application.

84.4. This fully automated process allows us to make decisions quickly, objectively, and continuously, based on pre-established and consistently applied credit risk assessment criteria. As this decision is made automatically, you are granted special rights and safeguards under the GDPR:

84.4.1.You have the right to contact us by email pagalba@paysera.lt to request information on the data used by the system to make the decision;

84.4.2.You may submit a new application after 14 days. This period is necessary to allow your financial data to update. When a new application is submitted, it will be assessed based on the most recent information.

85. Profiling for the purpose of anti-money laundering and terrorist financing:
85.1.We are legally obliged to carry out continuous and periodic monitoring of you and your transactions in order to prevent money laundering, terrorist financing, fraud, and other criminal activity.

85.2.For this purpose, we may use automated monitoring systems, including AI, which analyse your transaction data, behavioural patterns, and other information in real time. The system identifies unusual, suspicious, or non-compliant activity (e.g., unusually large transactions, dealings with high-risk jurisdictions, sudden changes in your behaviour).

85.3.If the system identifies potentially suspicious activity, this does not trigger an automatic decision that would have direct legal consequences for you. Instead, the system generates an alert, which is always reviewed and further investigated by our specialists. Only after human analysis can decisions be made, such as suspending a transaction, requesting additional information from you, or notifying law enforcement authorities.

86. Profiling for the purpose of service personalisation, marketing, and statistical analysis:
86.1.In order to enhance your experience, provide you with more relevant offers, and improve our services, we may carry out profiling.

86.2.Based on your consent, we may analyse your use of our services and behaviour to group you into specific Client segments. This allows us to send you personalised marketing messages and offers that we believe may be relevant to you. We may also utilise third-party platforms for this purpose (e.g., Google, Meta, OpenAI).

87. Based on our legitimate interest in developing and improving our business, we may analyse anonymised or aggregated data on how clients use our services. This helps us understand trends, identify areas for improvement, and develop new services.
88. You have the right to object at any time, without giving a reason, to the processing of your data for direct marketing purposes (including profiling). You also have the right to object to the processing of your data for statistical analysis. You can exercise these rights by changing the settings in your account, clicking the opt-out link in marketing messages, or contacting us directly.

Processing the personal data of minors

89. A minor under 14 (fourteen) years of age, seeking to use the payment services of Paysera, shall provide written consent from their representative (parent or legal guardian) with regard to their personal data processing.

Cookie policy

90. Paysera may use cookies on this website. Cookies are small files sent to a person's Internet browser and stored on their device. Cookies are transferred to a personal computer upon first visiting the website.
91. Usually, Paysera uses only the necessary cookies on the person's device for identification, enhancement of the website functionality and use, and facilitating a person's access to the website and the

information it contains. Paysera may use other cookies upon receiving the client's consent. You will find a brief description of different types of cookies here:
91.1.Strictly necessary cookies. These cookies are necessary in order for you to be able to use different features on the Paysera website. They are essential for the website to work and cannot be switched off. They are stored on your computer, mobile phone or tablet while you are using the website and are only valid for a limited amount of time. They are usually set in response to actions made by you while browsing such as changing your privacy settings, logging in and filling out various forms.

91.2.Statistics cookies. These cookies are used to collect and report on anonymous information in order to find out how our visitors use the website. A registered IN number is used to gather statistical data on how users navigate the website.

91.3.Analytics cookies. These cookies are used to monitor the number and traffic of website users. Analytics cookies help us find out which websites are visited the most and how visitors use them to improve the quality of our services. If you do not consent to the use of these cookies, we will not include your visit to our statistics.

91.4.Marketing cookies. These cookies are used to provide relevant information about our services based on your browsing habits to improve content selection and offer more options while using our website. In addition, these cookies may be used in our third-party partners' websites for reporting purposes. In that way, we would also receive information about your browsing history from our official partners' websites where we place our ads. If you do not consent to the use of these cookies, you will only see non-personalised advertising.

92. Most web browsers accept cookies, but the person can change the browser settings so that cookies would not be accepted. It should be noted that unlike other types of cookies, rejecting necessary cookies may affect the website functionality, and some features may not work properly. Upon first visiting the Paysera website, you will see a pop-up message with a list of specific types of cookies you may choose to accept or decline. If you decide to accept the necessary and the other types of cookies, you can change your selection and revoke your consent by clicking on Cookies Settings at the bottom of the page.

The right of access, rectification, erasure of your personal data, and to restrict data processing

93. You have the following rights:
93.1.The right of access to data. To obtain information as to whether or not Paysera processes your personal data, and, where that is the case, access to the personal data processed by Paysera and to receive information on what personal data and from which sources are collected, the purposes of the processing, the recipients to whom the personal data have been or may be provided; to obtain from Paysera a copy of the personal data undergoing processing in accordance with the applicable law. Upon the receipt of your written request, Paysera, within the time limit laid down in the legislation, shall provide the requested data in writing, or specify the reason of refusal. Once in a calendar year, data may be provided free of charge, but in other cases, remuneration may be set at a level not exceeding the cost of the data provision. More information on the right of access to data and its processing can be found here.

93.2.The right of rectification. If your data processed by Paysera is incorrect, incomplete, or inaccurate, you can address Paysera in writing for the rectification of the incorrect or inaccurate data or to have the incomplete personal data completed by providing a relevant request.

93.3.The right to be forgotten. To request the termination of the data processing (erase the data), when that the Data Subject withdraws the consent on which the processing is based, or the personal data is no longer necessary in relation to the purposes for which it was collected, or the personal data has been unlawfully processed, or the personal data has to be erased for compliance with a legal obligation. A written notice of objection to personal data processing shall be submitted to Paysera personally, by post, or via electronic means of communication. If your objection has legal grounds, Paysera, after examining the request, shall terminate any actions of processing of your personal data, with the exception of cases provided for by law. It should be noted that the right to require the immediate erasure of your personal data may be limited due to the obligation of Paysera as a payment service provider to store data about the clients' identification, payment transactions, concluded agreements, etc. for the period laid down in legislation.

93.4.The right to restrict the processing of data. To request to restrict the processing of personal data, when the accuracy of the personal data is contested by the Data Subject, for a period enabling the Data Controller to verify the accuracy of the personal data; the processing is unlawful, and the Data Subject opposes the erasure of the personal data and requests the restriction of its use instead; the Data Controller no longer needs the personal data for the purposes of the processing, but it is required by the Data Subject for the establishment, exercise, or defence of legal claims. A Data Subject who has obtained restriction of processing shall be informed by the Data Controller before the restriction of processing is lifted.

93.5.The right to object. The right to object to the processing of your personal data for direct marketing purposes.

93.6.The right to make a complaint. To address the supervisory authority with a claim regarding the processing of your personal data, if you believe that the personal data is processed in violation of your rights and legitimate interests stipulated by applicable legislation.

93.7.The right to contact the Data Controller and/or the Data Protection Officer for the purpose of exercising your rights.

93.8.Other rights established by law.

94. You can send your request for access, rectification, or objection to data processing via email to: dpo@paysera.com. The person submitting the request must clearly indicate their full name and sign the request with a qualified electronic signature.

Third-party websites

95. Paysera is not responsible for protecting the client's privacy on websites of third parties, even if the Client accesses such websites through links provided on this website. Paysera recommends learning the privacy policies of each website that does not belong to Paysera.

The use of logos

96. The client, using the services of Paysera for business objectives and professional interests, agrees that Paysera may use their name and/or logo for direct marketing purposes (e.g. by indicating that the Client is using the services provided by Paysera).

Ensuring Information Security

97. Paysera aims to ensure the highest level of security for all information obtained from the Client and public data files. In order to protect this information from unauthorised access, use, copying, accidental or unlawful erasure, alteration, or disclosure, as well as from any other unauthorised form of processing, Paysera uses appropriate legal, administrative, technical, and physical security measures.

Final Provisions

98. Additional information on how Paysera processes personal data may be provided in contracts, other documents, the website, mobile application or remote Client support channels (by phone, email, etc.).
99. Paysera has the right to unilaterally amend and/or supplement this Privacy Policy. Information about changes to the Privacy Policy is announced by publishing it on the Paysera website. In certain cases, Paysera may also inform individuals about the changes by mail, email, mobile application or in another manner.
100. These Privacy policy provisions are subject to the law of the Republic of Lithuania. All disputes regarding the provisions of the Privacy Policy shall be settled by negotiation and, in case of failure to resolve an issue by negotiation, the dispute shall be taken to courts of the Republic of Lithuania.

* – UAB "Creditinfo Lithuania" (company code: 111689163, address: Lvivo st. 21A, LT-09309 Vilnius, Lithuania, www.creditinfo.lt, phone: (8 5) 2394131, and UAB "Okredo", company code: 304106783, address: Liepų st. 54-1, Klaipėda, Lithuania, which manages and provides your information to third parties (financial institutions, telecommunication agencies, insurance, electricity and utility service providers, trading companies, etc.). We collect and provide your information for legitimate interests and objectives: to assess your creditworthiness and manage debts. Credit history data is usually stored for 10 (ten) years after the fulfilment of obligations).

Using services provided solely by "Paysera Bank of Georgia", JSC, personal data collected through "Paysera Bank of Georgia", JSC is processed under this Privacy Policy.

Agreement History

Privacy Policy (valid until 17/06/2024)

Privacy Policy (valid until 28/09/2021)

Privacy Policy (valid until 20/07/2020)

Privacy Policy (valid until 17/04/2020)

Privacy Policy (valid until 16/09/2019)

Privacy Policy (valid until 01/01/2026)