Published on: 30/12/2025

# Privacy Policy

## General definitions

1. **Personal data** – any information relating to an identified or identifiable natural person (“Data Subject”); an identifiable natural person is one who can be identified directly or indirectly, in particular through an identifier such as the name, identification number, location data, online identifier, or one or more specific factors of the physical, physiological, genetic, mental, economic, cultural, or social identity, according to the definitions of Law no. 124/2024 “On the protection of personal data”.
2. **Law** – Law no. 124/2024 “On the protection of personal data”, as well as the by-laws issued for its implementation. Regulation (EU) 2016/679 of the European Parliament and of the Council, dated 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”, as well as the repeal of Directive 95/46/EC.
3. **Data processing** – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure through transmission, publication or making available in any other manner, alignment or combination, restriction, erasure, or destruction.
4. **Data Processor** – any natural or legal person, public authority, agency, or other body which processes personal data on behalf of and according to the instructions of the Data Controller, in accordance with Law no. 124/2024 “On the protection of personal data”.
5. **Data Controller** – the entity that determines the purposes and means of the processing of personal data is Paysera Albania LLC, which manages the payment initiation service and account information service, qualified electronic identification, and other services. The contact details of Paysera Albania are published on the Paysera website www.paysera.al. Paysera Albania LLC, NUIS/NIPT M01608007N, with headquarters at “Fadil Rada” Street, Donika Building, Floor 3, Tirana, Albania. The contact details of the Data Protection Officer appointed by Paysera are: dpo@paysera.al.
6. **Joint Data Controller** – Your controller of personal data is the Paysera network. According to the Joint Controller Agreement No. 2018019 dated 19/09/2018, Paysera Albania together with the other companies of the network and with the coordinator Paysera Tech, acts as a Joint Controller in accordance with Annex No. 16 “Network Agreement on Data Governance” of the Joint Activity Agreement. This agreement regulates the division of responsibilities and ensures data protection within the network. Personal data are jointly processed only in order 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 to ensure uninterrupted customer support when services are provided by another network partner.
7. **Data Subject or Client** – a natural person who intends to enter, or has entered, into a business relationship with the Data Controller (e.g., creation of a profile, opening of a payment account, obtaining

a qualified electronic identification tool, entering into a service provision agreement with the Company, etc.), or whose business relationship has ended, but whose data are still processed by the Data Controller in accordance with legal provisions.

8. **Platform** – a software solution hosted on the 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 are processed in accordance with Law no. 124/2024 "On the protection of personal data" of the Republic of Albania, the GDPR, as well as the by-laws issued for its implementation. All persons, representatives, and employees of representatives acting on behalf of Paysera who have the ability to access systems containing Client data, access them exclusively for the performance of their work functions, having a legitimate basis for such access, and must keep the personal data learned during work confidential even after the termination of employment or contractual relationships.
10. The Company, in accordance with applicable legal requirements, shall ensure the confidentiality of personal data and the implementation of appropriate technical and organizational measures to protect personal data from unauthorized 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, as well as other information related to you, including the scope, purpose, sources, recipients, and other important aspects of the processing of your personal data when you use Paysera as a payment service provider. In this Privacy Policy, terms used in the singular include the plural form, and terms used in the plural include the singular form, unless the context clearly indicates otherwise.
12. By accessing the Paysera website and/or using the application, and/or the information contained therein, and/or the services, you acknowledge and confirm that you have read, understood, and agree to this Privacy Policy. Furthermore, once you register in the system and begin using Paysera services, this Privacy Policy becomes an Annex 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, by notifying registered users via email or in-app notification. A revised or updated version of this Privacy Policy shall become effective upon its publication on the website.
14. If the service user is a business client, this Privacy Policy also applies to natural persons whose personal data are transferred to Paysera by the business client, including administrators, partners, legal representatives, employees, beneficial owners, agents, or other persons associated with the business client. The business client undertakes to inform these Data Subjects about the transfer and processing of their personal data by Paysera, in accordance with Law no. 124/2024 "On the protection of personal data" and Article 14 of the GDPR.

## Purposes of data processing, providers, retention periods, recipients

15. The main purpose for which Paysera collects your personal data is to provide Paysera payment services to clients who send and receive payments. As a payment service and qualified electronic identification provider, Paysera is legally obliged to determine and verify your identity before entering into financial service transactions with you. Furthermore, during the provision of services, it is required to request additional information, as well as to assess and retain this information for the retention period defined by law. In view of this, you must provide accurate and complete information.

**PURPOSE: Customer identification, provision of payment services (opening an account, fund transfers, payment processing, etc.), qualified electronic identification services, prevention of money laundering and terrorist financing, submission of reports to state authorities, and compliance with other legal obligations of the payment service provider.**

16. Personal data are processed for this purpose in accordance with the legal requirements related to: customer identification and identity verification; entering into and performing agreements with the Client, as well as taking pre-contractual measures at the Client's request before concluding an agreement; execution of fund transfers and transmission of necessary information accompanying the transfer in accordance with applicable legislation; compliance with "Know Your Customer" ("KYC") requirements; ongoing and periodic monitoring of client activity; risk assessment; updating Client data to ensure its accuracy; prevention of money laundering and terrorist financing; prevention of fraud, detection, investigation, and reporting of such activities; identification of politically exposed persons (PEPs) or financial sanctions applied to the client; as well as ensuring proper risk management and internal organization.
17. For this purpose, the following personal data may be processed: name, surname, gender, personal identification number, date of birth, facial photograph, live video transmission recording (live video stream), nationality, place of birth, place of residence, identity document data (including but not limited to a copy of the document), address, email address, phone number, current payment account number, IP address, current professional or employment 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-terrorism financing laws, as well as the Client's location data, planned service, purpose of account use (personal/business), planned investment amount, income received, main source of funds, origin of funds, beneficial owner, information about the ultimate beneficial owner: name, surname, nationality, personal identification number (national ID number), date of birth, address, authorization basis, political exposure, other data specified in the Client "Know Your Customer" (KYC) questionnaire, correspondence within the business relationship with the client, documents and data confirming a monetary operation or transaction, or other legally valid documents and data related to the execution of monetary operations or transactions, tax residence country, connection to 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 address, system language of the device, SIM card issuing country, SIM card operator, pseudo-unique device ID, Android ID, Android GSFID, Android fingerprint, web-view version, Paysera application version, and transaction history.
18. These personal data are collected and processed in the performance of public authority functions assigned to the Data Controller, and on the basis of a legal obligation imposed on the payment service provider, namely Law no. 55/2020 "On payment services", legislation on electronic money institutions and financial institutions, Law no. 9917, dated 19.05.2008 "On the prevention of money laundering and terrorist financing", as amended, as well as any other applicable legal and sub-legal acts in the Republic of Albania, and are required for the purpose of opening an account and/or providing a payment service.
19. **Data retention period:** The retention period for personal data is 10 (ten) years after the termination of the business relationship with the client. Personal data are stored for 5 (five) years in accordance with Law no. 9917, dated 19.05.2008 "On the prevention of money laundering and terrorist financing", as amended, and the by-laws implementing it. After the end of this period, the data may be retained for an additional period where necessary for the protection of Paysera's legitimate interests, for the exercise or defense of legal claims, as well as in accordance with the limitation periods provided for by applicable Albanian legislation.
20. Providers and sources of personal data:
21. The Data Subject, directly;

    21.1. Third parties, including but not limited to:

21.1.1. Banks, financial institutions, payment institutions, electronic money institutions, and their branches or partners;

21.1.2. Public and private registers, state or commercial databases;

21.1.3. Databases for verifying identity documents and their authenticity, including international databases of lost, stolen, or expired documents;

21.1.4. Registers and databases of authorizations, legal representation, powers of attorney, or notarial verifications;

21.1.5. Public registers containing data on restrictions on legal capacity or other legal measures applicable to individuals;

21.1.6. The National Civil Status Register and other state or private databases permitted by applicable legislation;

21.1.7. Entities providing credit information services, risk assessment services, or financial liability history management;

21.1.8. Entities managing or providing access to international sanctions databases, lists of politically exposed persons (PEPs), and watchlists.

21.1.9. Law enforcement authorities, supervisory authorities, public bodies, and competent institutions;

21.1.10. Judicial enforcement officers and debt enforcement authorities;

21.1.11. Legal entities with which the Data Subject has a relationship as a legal representative, employee, partner, shareholder, administrator, contractor, or beneficial owner;

21.1.12. Business partners, service providers, or other legal entities involved in the provision of services.

21.1.13. Social networks or electronic platforms, when the Data Subject chooses to link their profile with our systems or services;

21.1.14. Other lawful sources, in accordance with applicable Albanian legislation and the GDPR.

22. For the purpose of more effective fulfilment of our legal obligations—for example, to identify potentially suspicious financial transactions for the purposes of preventing money laundering or to verify the authenticity of identity documents—we may use artificial intelligence (AI) solutions (the tools may be trained using existing data, or data may be analysed by the tools). These tools help process large volumes of data and/or identify inconsistencies; however, any final decision that may or may not have significant consequences for you is always reviewed and approved by our employees.
23. **Categories of data recipients:** supervisory authorities; banks; financial institutions; payment institutions; electronic money institutions and their branches or partners; pre-trial investigation and prosecution authorities, including the State Police, the Prosecutor’s Office, and other competent law enforcement authorities; as well as the Albanian Tax Administration (General Directorate of Taxes and its

subordinate structures), in accordance with applicable Albanian legislation; payment service representatives or Paysera partners (if the transaction is carried out using their services); recipients of transaction funds who receive information in payment statements together with the transaction funds; the recipient's payment service providers and correspondent institutions; participants and/or related parties in national, European, and international payment systems; debt collection agencies, including any company licensed or authorised under Albanian law to carry out debt management, recovery, and collection services; companies or entities processing and managing credit history and financial liability data (credit information companies), in accordance with applicable Albanian legislation; lawyers, bailiffs, auditors; other entities having a legitimate interest; and other persons pursuant to an agreement with Paysera or on other legal grounds.

**PURPOSE: Dispute and debt management.**

24. Personal data are processed for this purpose in order to resolve disputes, manage and collect debts, and to bring and/or defend claims, demands, lawsuits, and other legal or administrative proceedings.
25. For this purpose, the following categories of personal data may be processed: name, surname, personal identification number, residential and/or correspondence address, date of birth, identity document data, email address, phone number, bank account number, IP address, bank account statements and extracts, recordings audio and video recordings, as well as any other personal data directly related to the circumstances giving rise to the dispute or financial obligation.
26. **Personal data retention period:** Personal data are stored until the expiry of the limitation period for the relevant obligation, which, in the case of financial claims, is 10 (ten) years from the date on which the obligation becomes due and payable (in the case of instalment obligations, from the due date of the last instalment). In the event of the initiation of court or enforcement proceedings, data are stored until the full completion of such proceedings and the full fulfilment of obligations between the parties, but not less than the statutory limitation period. The retention periods are based on the relevant provisions of the Civil Code of the Republic of Albania and applicable legislation on limitation of claims.
27. **Sources of data:** the Data Subject (directly), financial, banking and payment institutions, public institutions and state and/or private registers, companies managing and processing debtor registers and credit assessment, electronic communications service providers, as well as any other lawful source in accordance with Albanian legislation.
28. **Categories of data recipients:** financial and payment institutions, banks, credit management and/or credit risk assessment companies, lawyers, private bailiffs, courts and other bodies of the justice system, investigative authorities and tax authorities, as well as debt collection companies and any other party having a legitimate interest in accordance with Albanian legislation.
29. Please note that in the event you have outstanding obligations towards the company and delay their fulfilment, the company has the right, in accordance with applicable Albanian data protection legislation and applicable civil and financial legislation, to share certain identifying and financial data (such as identity data, contact details, and information on financial obligations and payment history) with companies that manage credit and debtor databases, as well as with companies licensed for debt collection. The Data Subject has the right to access their credit information through such companies in accordance with their internal procedures and applicable law.

**PURPOSE: Customer relationship support and administration, informing clients about existing and new services, provision of services, prevention of disputes and collection of evidence (recording of telephone conversations), and correspondence within the business relationship with the Client.**

30. Personal data are 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 and ensure evidence of business communication with the Client (call recordings, correspondence); perform service quality assessment and ensure the quality of services provided by Paysera; where necessary for the performance of the agreement, in order to take steps at the Client's request or to comply with a legal obligation; inform the Client about Paysera's services, their

prices, specifications, changes to contracts concluded with the Client, etc.; send system notifications from Paysera and other notifications related to the services provided.

31. 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, telephone call recordings, correspondence with the Client, and any other data necessary for this purpose.
32. The personal data retention period is 10 (ten) years after the termination of the business relationship with the client. Personal data are stored for 5 (five) years in accordance with Law no. 9917, dated 19.05.2008 “On the prevention of money laundering and terrorist financing”, as amended, and the by-laws implementing it. After the end of this period, the data may be retained for an additional period where necessary for the protection of Paysera’s legitimate interests, for the exercise or defence of legal rights, as well as in accordance with the limitation periods provided for by applicable Albanian legislation.
33. **Data providers:** the Data Subject directly, electronic communications service providers.
34. **Data recipients:** law enforcement authorities, supervisory authorities, public bodies and competent institutions, lawyers, bailiffs, debt collection and recovery agencies, other entities having a legitimate interest, and other entities pursuant to an agreement with Paysera.
35. The Data Subject confirms that they understand that such informational notifications are necessary for the performance of the General Payment Services Agreement and/or its annexes related to the Client, and do not constitute direct marketing messages.

**PURPOSE: Provision of services through third parties**

36. Personal data for this purpose are processed in order to ensure the widest possible range of services received by Paysera clients, with certain services being provided by third parties.
37. For this purpose, the following personal data may be processed: name, surname, nationality, personal identification number, address, contact information.
38. The Client is clearly informed about any processing of data for the purpose of providing services through third parties, and the data are processed only with the Client’s explicit consent.
39. **Data retention period:** 1 (one) year.
40. **Data providers:** the Data Subject directly, Paysera, third parties providing services.
41. **Data recipients:** third parties providing services, Paysera, the Data Subject.

**PURPOSE: Protection and safeguarding of Paysera’s and the Client’s interests (video surveillance in Paysera premises).**

42. Personal data are processed for this purpose on the basis of legitimate interests under Law no. 124/2024. These interests include security, including the protection of the health, life, and property of employees, as well as ensuring a safe and secure working environment for Clients and other visitors against unlawful acts such as theft, vandalism, or physical attacks; the protection of legal rights and legitimate interests (collecting objective evidence for the investigation of incidents, accidents, or disputed situations); and ensuring the accuracy and transparency of services.
43. For this purpose, the following personal data may be processed: video recordings in premises managed by Paysera.
44. Video surveillance is carried out in a limited area of Paysera’s premises, including only the entrance area to Paysera’s office, with the aim of ensuring internal order and property security. Before entering Paysera’s premises where video surveillance is conducted, you are informed about the surveillance through special signs.
45. Video recordings at the entrance of the Paysera office are stored for 72 hours. This retention period is necessary to ensure the ability to detect and investigate incidents within a reasonable timeframe, to resolve urgent disputes, and to comply with law enforcement data requests. After this period, the data are deleted, unless they are required for an ongoing investigation, dispute resolution, or other cases provided for by law—in which case they are retained for as long as necessary to achieve these purposes.

46. **Data providers:** the Data Subject directly, who visits Paysera's premises where video surveillance is carried out and is captured by the surveillance camera.
47. **Data recipients:** video recordings are treated as confidential. Access is strictly limited and granted only to employees who need it for the performance of their job functions (the "need-to-know" principle) and solely for the purposes described above. Recordings may also be disclosed to courts, pre-trial investigation and prosecution authorities (State Police, the Prosecutor's Office, and other competent law enforcement authorities). Internal review of recordings is carried out only when there is a clear need—for example, when investigating an incident or resolving a dispute, etc.

**PURPOSE: Direct marketing.**

48. For this purpose, personal data are processed in order to provide clients with offers regarding services offered by Paysera and to obtain clients' feedback on the above-mentioned services.
49. The following personal data may be processed for this purpose: name, surname, email address, and phone number.
50. For this purpose, Paysera sends newsletters and direct marketing messages after obtaining the Client's consent. Paysera may use a newsletter service provider, ensuring that the said provider complies with the personal data protection requirements set out in the Joint Controller Agreement. The Client may withdraw their consent after receiving newsletters or direct marketing messages by clicking the "Withdraw your consent" link, as well as by informing Paysera at any time of their refusal to process personal data for direct marketing purposes via email at support@paysera.al.
51. **Data retention period:** until the termination of the business relationship with the Client or until the day the Client objects to the processing of data for this purpose.
52. **Data providers:** the Data Subject directly.
53. **Data recipients:** data for this purpose may be transmitted to search engines or social networks (the option to object to data processing is provided by the websites of these systems), and newsletter service providers.

**Purpose: statistical analysis, service improvement.**

54. Your personal data collected and anonymised for the above-mentioned purposes may be processed under Law no. 124/2024 for the purpose of statistical analysis and improving technical and organisational measures, information technology infrastructure, ensuring the adaptation of the service provided to the devices used, creating new Paysera services, increasing satisfaction with existing services, and testing and improving technical measures and IT infrastructure. For this purpose, personal data will be processed in such a way that, by including them within the scope of statistical analysis, it is not possible to identify the respective Data Subjects. The collection of your personal data for statistical analysis purposes is based on legitimate interest in analysing, improving, and developing the business activity.
55. You have the right to object to the processing of your personal data for such purpose at any time and in any form by informing Paysera accordingly. However, Paysera may continue to process the data for statistical purposes if it demonstrates that the data are processed for compelling legitimate reasons that override the interests, rights, and freedoms of the Data Subject, or for the establishment, exercise, or defence of legal claims.

**Purpose: Prevention of misuse of services and criminal offences, as well as ensuring the proper, accurate, and secure provision of services.**

56. The data collected for all the above purposes may be used to prevent unauthorized access and use, i.e. to ensure the privacy and security of information.
57. For the processing of personal data, Paysera may engage Data Processors and/or, at its discretion, employ other persons to perform certain supporting functions on behalf of Paysera (e.g. data centres, hosting, cloud hosting, system administration, system development, software development, provision

and support services such as improvement and development; customer service centre services; marketing, communication, consultancy, temporary employment 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 appropriate personal data security measures. Paysera shall also ensure that such persons are bound by confidentiality obligations and may not use this information for any purpose other than the performance of their functions.

58. Personal data collected for the purposes set out in this Privacy Policy shall not be processed in a manner incompatible with those purposes or with applicable legal requirements, in accordance with the principles of data protection legislation.
59. The data referred to above will be provided and obtained through a software tool used by Paysera or its authorised agent, as well as through other means and third parties with whom Paysera has concluded agreements for the processing of personal data in accordance with applicable laws and regulations.

## Geographical area of processing

60. In general, personal data are 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 adequacy decision by the European Commission are carried out in accordance with the Network Agreement on Data Governance. This agreement ensures the automatic application of the Standard Contractual Clauses (SCCs) adopted by the European Commission for all data transfers between network members, guaranteeing that your data is protected in accordance with GDPR requirements, regardless of the partner's location.
61. Your personal data may be transferred to the following categories of recipients in Third Countries:
    1. For infrastructure and platform partners. Our services are provided using the shared IT infrastructure of the Paysera network, which is managed and maintained by our strategic partner. Although this partner operates through a holding company registered in the European Union, its primary country of registration is the Cayman Islands. Please note that the technical access and administrative data necessary to ensure the operation, security, and maintenance of the platform are not accessible from this jurisdiction, and all data are stored within the EU/EEA territory. Data transfers to Third Countries that do not have an adequacy decision from the European Commission are carried out in accordance with a Joint Activity Agreement, which provides for the automatic application of the Standard Contractual Clauses (SCCs) adopted by the European Commission for all data transfers between network partners. This ensures that your data is protected in accordance with GDPR requirements, regardless of the partner's location.
    2. Paysera network partners. We operate as part of an international corporate network. When you use services involving our partners, or your transactions are linked to them, your data may be transferred to these partners, who operate in Third Countries such as the Republic of Kosovo, Georgia, and others.
    3. External service providers and specialists. To ensure uninterrupted 24/7 high-quality customer 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 specific functions assigned to them (e.g. verifying documents you have submitted or responding to your inquiries).
    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.

62. Since the above-mentioned Third Countries are not required to apply EU-level data protection standards, one or more of the safeguards provided under the GDPR are applied to each data transfer:
    1. Standard Contractual Clauses (SCC). For all data transfers related to the system within Paysera's infrastructure, we have concluded Standard Contractual Clauses (SCC) with data recipients for the transfer of personal data to Third Countries, as adopted by the European Commission. These agreements legally bind the data recipients to process your data in accordance with EU data protection standards.
    2. Additional technical and organisational measures have been implemented, such as 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 access the data, and contractual obligations requiring the data recipient to promptly inform us of any requests from authorities to disclose data and to legally challenge such requests where possible.
63. For international payments initiated by you, the transfer of personal data is based on the derogations provided under Law no. 124/2024 "On the protection of personal data", specifically the provisions on international data transfers, as such transfer is necessary for the performance of the agreement between you and us, including the execution of the payment transfer instructed by you, in accordance with Article 41, paragraph 3, point (b) of the law, as well as Article 49 of the GDPR.

## Profiling and Automated Decision-Making

64. To provide you with fast, secure, and modern services and to comply with our legal obligations, we use advanced technologies, including automated systems and artificial intelligence (AI) solutions. These technologies help us automatically process your personal data to assess certain personal characteristics (profiling) and, in some cases, to make decisions without direct human intervention (automated decision-making).
65. This fully automated process allows us to make decisions quickly, objectively, and consistently. Since this decision is made automatically, you are granted specific rights and safeguards under the GDPR.

65.1. You have the right to contact us by email at dpo@paysera.al to request information about the data used by the system to make the decision;

66. Profiling for the purpose of preventing money laundering and terrorist financing:

66.1. We are legally obliged to carry out ongoing and periodic monitoring of you and your transactions for the purpose of preventing money laundering, terrorist financing, fraud, and other criminal activities.

66.2. For this purpose, we may use automated monitoring systems, including AI, which analyses your transaction data, behavioral patterns, and other information in real time. The system identifies unusual, suspicious, or inconsistent activity (e.g., unusually large transactions, relationships with high-risk jurisdictions, sudden changes in your behavior).

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

67. Profiling for the purpose of service personalization, marketing, and statistical analysis:

67.1. In order to improve your experience, provide you with more relevant offers, and enhance our services, we may carry out profiling.

67.2. Based on your consent, we may analyses your use of our services and your behavior in order to group you into specific customer segments. This allows us to send you marketing messages and personalized offers that we believe may be relevant to you. We may also use third-party platforms for this purpose (e.g., Google, Meta, OpenAI).

68. 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.
69. You have the right to object at any time, without providing a reason, to the processing of your personal data for direct marketing purposes (including profiling). You also have the right to object to the processing of your personal data for statistical analysis. You may exercise these rights by changing the settings in your account, clicking the opt-out link in marketing messages, or contacting us directly.

## Cookies Policy

70. Paysera may use cookies on its website. Cookies are small files sent to a person’s web browser and stored on their device. Cookies are transmitted to a personal computer after the first visit to the website.
71. Generally, Paysera uses only necessary cookies on a person’s device for identification, improving the functionality and usability of the website, and facilitating a person’s access to the website and the information it contains. Paysera may use other cookies after obtaining the Client’s consent. You will find a brief description of the different types of cookies here:

**7**1.1**.** Strictly necessary cookies. These cookies are required in order for you to be able to use various features on the Paysera website. They are essential for the website to function and cannot be turned off. They are stored on your computer, mobile phone, or tablet while you are using the website and are valid only for a limited period of time. They are usually set in response to actions taken by you while browsing, such as changing your privacy settings, logging in, and filling in various forms.

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

71.3. Analytics cookies. These cookies are used to monitor the number of users and traffic on the website. Analytics cookies help us determine which web pages are visited most and how visitors use them, with the aim of improving the quality of our services. If you do not consent to the use of these cookies, we will not include your visit in our statistics.

71.4. Marketing cookies. These cookies are used to provide relevant information about our services based on your browsing habits, with the aim of improving content selection and offering more options while using our website. In addition, these cookies may be used on our third-party partner websites for reporting purposes. In this way, we may also receive information about your browsing history from our official partner websites where we place our advertisements. If you do not consent to the use of these cookies, you will only see non-personalized advertising.

72. Most web browsers accept cookies, but a person can change their browser settings so that cookies are not accepted. It should be noted that, unlike other types of cookies, refusing necessary cookies may affect the functionality of the website, and some features may not work properly. After your first visit to

the Paysera website, you will see a pop-up message with a list of specific cookie types that you can choose to accept or refuse. If you choose to accept necessary cookies and other types of cookies, you may change your selection and withdraw your consent by clicking “Cookies Settings” at the bottom of the page.

**Right of access, rectification, erasure of your personal data, and restriction of processing**

73. You have the following rights:

73.1. **Right of access to data.** To obtain information on whether Paysera processes your personal data, and where applicable, access to the personal data processed by Paysera and information on which personal data and from which sources are collected, the purposes of processing, and the recipients to whom the personal data have been or may be disclosed; to receive from Paysera a copy of the personal data undergoing processing in accordance with applicable law. Upon receipt of your written request, Paysera shall, within the timeframe specified by law, provide the requested data in writing or specify the reason for refusal. Once per calendar year, the data may be provided free of charge; however, in other cases, a fee may be applied at a level not exceeding the cost of providing the data. More information about the right of access to data and their processing can be found here.

73.2. **Right to rectification.** If your personal data processed by Paysera are inaccurate, incomplete, or incorrect, you may submit a written request to Paysera to correct inaccurate or incorrect data, or to complete incomplete personal data.

73.3. **Right to be forgotten.** To request the cessation of processing of data (deletion of data) when the Data Subject withdraws consent on which the processing is based, or when the personal data are no longer necessary in relation to the purposes for which they were collected, or when the personal data have been unlawfully processed, or when the personal data must be erased to comply with a legal obligation. A written notice of objection to the processing of personal data shall be submitted to Paysera in person, by post, or via electronic means of communication. If your objection has legal grounds, Paysera, after reviewing the request, shall stop any processing of your personal data, except in cases provided by law. It should be noted that the right to request immediate deletion of your personal data may be limited due to Paysera’s obligation as a payment service provider to retain data on customer identification, payment transactions, concluded contracts, etc. for the period specified in legislation.

73.4. **Right to restriction of processing.** To request the restriction of processing of personal data where 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; where the processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of its use instead; where the Data Controller no longer needs the personal data for the purposes of processing, but they are 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.

73.5. **Right to object.** The right to object to the processing of your personal data for direct marketing purposes.

73.6. **Right to lodge a complaint.** To contact the supervisory authority at info@idp.al— the Information and Data Protection Commissioner’s Office (Zyra e Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale) — www.idp.al, with a complaint regarding the processing of your personal data, if you believe that your personal data are being processed in violation of your lawful rights and interests as provided by applicable legislation.

73.7. **Right to contact the Data Controller** and/or the Data Protection Officer in order to exercise your rights.

73.8. Other rights provided by law.

74. You may submit your request for access, rectification, or objection to data processing via email at: dpo@paysera.al. The person submitting the request must clearly state their full name and sign the request with a handwritten signature or a qualified electronic signature.

**Third-party websites**

75. Paysera is not responsible for the processing of personal data or the protection of privacy on third-party websites, platforms, or services, even in cases where access to such sites is provided through links published on Paysera's website or applications. Paysera recommends that the Client review in advance the privacy policies and terms of use of any third-party website or service before using them.

**Use of logos**

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

**Information Security**

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

**Final Provisions**

78. Additional information on how Paysera processes personal data may be provided in contracts, other documents, the website, the mobile application, or the Client's remote support channels (by phone, email, etc.).
79. Paysera has the right to unilaterally amend and/or supplement this Privacy Policy. Information about changes to the Privacy Policy shall be published on Paysera's website. In certain cases, Paysera may also inform individuals about changes by post, email, mobile application, or by other means.
80. These provisions of the Privacy Policy shall be governed by and interpreted in accordance with the legislation of the Republic of Albania. Any dispute arising in connection with the interpretation, implementation, or validity of this Privacy Policy shall first be resolved amicably between the parties through negotiations. If the dispute cannot be resolved by mutual agreement, it shall be submitted to the jurisdiction of the competent courts of the Republic of Albania.

Privacy Policy (Valid until 30/12/2025)

Privacy Policy (valid until 18/06/2021)