NovaPay

Privacy Policy

Version v1.2

2025

Contents

Versioning:

Current version applicable as of: 26 September 2025

Previous versions:

- *Version dated 01 February 2025;*
- *Version dated 03 July 2025*

1 Purpose and Data Controller / Data Processor

This Privacy Policy (the **Policy**) outlines the types of personal data related to you (the **Data**) that we collect, process, and the legal basis for such processing when you use our mobile application ("**Mobile Application**") or our website https://novapay.com ("**Website**").

It also explains the purposes for which we use your Data, along with details about your rights and how to exercise them.

Please note: The Website is an informational resource designed to provide you with general information about NovaPay services and allow you to download the Mobile Application. You are not required to log in, register, or submit any personal information directly on the Website. We do not collect personal data via the Website except where strictly necessary (e.g., through the use of cookies or similar technologies as described in Section 9). Any such collection is minimal and based on your consent.

NovaPay EU UAB ("**NovaPay**", "**we"** or "**us**") will act as the '**controller**' or '**processor**' of your Data depending on the nature of the processing, as described below:

NovaPay EU UAB
Company code: 306126592
Email address: info.NovaPayEU@novapay.ua
Website address: https://novapay.com/ua

Mobile Application name: NovaPay
Mailing address: L. Stuokos-Gucevičiaus g. 7, LT-01122, Vilnius, Lithuania

For Data processed for the purposes of operating the Mobile Application and the Website – including ensuring their security, functionality, improvement, analytics and, where permitted, marketing activities – NovaPay acts as the **data controller**.

In relation to payment services offered through the Mobile Application, NovaPay EU UAB acts as a **data processor on behalf of Quicko**. Quicko sp. z o.o., authorised to provide payment services as a National Payment Institution licensed in the Republic of Poland, holding the license number IP52/2021, with its registered office in Tarnowskie Góry, at ul. Sienkiewicza 49, 42-600, registered in the Register of Entrepreneurs of the National Court Register kept by the District Court in Gliwice, 10th Commercial Division of the National Court Register, under the KRS number 0000350151, NIP 5213540295, REGON 142004870. Quicko is the **data controller** for payment services, and the processing of your Data for those services is governed by the Quicko Privacy Policy, which you can access **here**.

When processing Data in the EEA, we comply with the General Data Protection Regulation of the European Union (**GDPR**), the Law on Legal Protection of Personal Data of the Republic of Lithuania, and other directly applicable legal acts governing Data protection.

You can contact our Data Protection Officers via email at dpo@novapay.lt

2 Categories of Data we process

- **Identity Data:**

This includes your name, surname, personal identification number, photo, gender, country, city, date of birth, country/countries of residence, permanent address, and identity document details, including photo, expiration date, document copy, signature, nationality/nationalities, and taxpayer identification number.

- **Financial Transaction Data:**

This includes bank account number, payment type, payment purpose/payment name, transaction ID, payer code, payment code, time, amount, and location.

- **Your Account and Contact Data:**

This includes name, surname, email address, phone number, user ID, last login time, account creation and deletion dates, last account update date, usage habits, preferences for receiving notifications about unpaid bills, newsletters, and offers, confirmation of agreement with terms and conditions, account PIN code (processed securely for payment authorization), payment history, subscribed services, app login settings using biometric data, log records of actions performed on our Mobile Application, preferred language, and participation confirmations in promotional campaigns.

- **Device Data:**

This includes internet protocol (IP) address, browser type, time zone setting, model of your phone or mobile device, Geo-location, information about your visit on our Mobile Application, including log records of actions performed.

- **Data concerning implementation of Anti-Money Laundering and Terrorist Financing Prevention (AML/CTF) and International Sanctions measures:**

This includes name, surname, date of birth, personal identification number, identity document details, qualified signature data, transaction details (including amount, account, and transaction type), signature, phone number, email address, copy of identity document, personal photo, additional due diligence and business relationship monitoring data, information on received amounts, sanctions, and any other data necessary for compliance with anti-money laundering, counter-terrorist financing, tax evasion prevention,

and international sanctions implementation, information on PEP status: whether you or your family members or close associates are classified as politically exposed persons (PEPs).

- **Social Media Interaction Data:**

This includes username, post comments, shared posts, information on likes and follows, reactions to posts, photos, ratings, and any other information you provide.

- **Inquiry, Request, or Complaint Data:**

This includes data on your inquiries, requests, or complaint details, attached files, conversation recordings, call date and time, and call duration.

- **Legal Data:**

This includes documents and data with legal implications, communications, legal documents, procedural documents, attachments, court documents, investigation details, information on criminal convictions and offenses, and any other data submitted in legal proceedings.

Please note that the data categories as outlined above reflect the main types of Data we process. However, given the nature of our business, this Policy does not provide an exhaustive list of all possible data categories. As a result, the list is not definitive. The exact scope of Data processing depends on the services you use and your relationship with NovaPay.

3 What do we use your Data for?

Depending on the context, we process your Data either:

- as a data controller (for the purposes of operating our Mobile Application and Website), or
- as a data processor acting on behalf of Quicko (for the purposes of providing payment services through the Mobile Application).

We process your Data for the following purposes:

3.1 Signing you up as NovaPay Mobile Application customer

To enable you to create an account on our Mobile Application, we will process the following data.

• **Lawful Basis:**	Contract (GDPR Article 6(1)(b))
• **Data Category:**	Your Account and Contact Data
• **Optional or Mandatory:**	Mandatory. Failure to provide the data will prevent us from enabling your registration on our Mobile Application.

3.2 Identification and verification of your identity, implementation of AML/CTF and International Sanctions measures

To comply with the applicable laws, we must verify your identity for security and compliance reasons, including SEPA payments. This may require a photo of your ID, a selfie, and other necessary details.

• **Lawful Basis:**	Legal Obligation (GDPR Article 6(1)(c)) and Public Interest (GDPR Article 9(2)(g))
• **Data Category:**	Identity Data; Financial Transaction Data; Data concerning implementation of AML/CTF and International Sanctions measures.
• **Optional or Mandatory:**	Mandatory. Failure to provide the required data will prevent you from fully accessing our services (e.g., initiate payment transactions).

3.3 Organization of Promotions

When you participate in NovaPay promotions through Mobile Application, we will process the following data.

• **Lawful Basis:**	Consent (GDPR Article 6(1)(a))
• **Data Category:**	Your Account and Contact Data.
• **Optional or Mandatory:**	Optional. If you do not consent, NovaPay will be unable to include you in promotional activities, and you will not be able to access or participate in promotions organized by NovaPay.

3.4 Marketing

When you register on our Mobile Application, provide your consent, or when we have a legitimate interest, we may send you relevant offers, updates on our or our partners' services and products, and request your feedback on our services.

To withdraw your consent to receive marketing communications, you may do so at any time in one of the following ways:

- By clicking the **"Unsubscribe"** link in any marketing email you receive from us.
- Via the Mobile Application: go to **Profile → Terms & Tariffs → Marketing Consent**, then withdraw by turning off the switcher.
- Or by sending a request via email to cc@novapay.lt

• **Lawful Basis:**	Consent (GDPR Article 6(1)(a)); Legitimate interest in informing you about services and products (GDPR Article 6(1)(f)); Customer Relationship (Article 81(2) of the Electronic Communications Law of the Republic of Lithuania)
• **Data Category:**	Your Account and Contact Data.
• **Optional or Mandatory:**	Optional.

3.5 Customer Behavior and Habits Analysis

We use **Google Firebase Analytics** and **AppsFlyer,** to better understand how customers interact with our Mobile Application, allowing us to better meet their needs. This helps us enhance our products, services, and user experience while optimizing and refining our offerings.

We also perform profiling based on user activity and behaviour data to tailor our communication (e.g., push notifications, emails, SMS) and provide reminders about features that users have not yet tried or engaged with.

The profiling is used solely for improving user experience and tailoring communication. It does not result in decisions that produce legal or similarly significant effects for you, in accordance with GDPR Article 22(1).

When you use our Website, we use cookies (see Section 9), to collect data about how visitors interact with the site. This helps us analyze usage patterns, improve website performance, and measure the effectiveness of marketing campaigns. For example, we may assess which pages users visit most or which ads lead to clicks.

• **Lawful Basis:**	Legitimate interest in understanding customer needs and meeting expectations (GDPR Article 6(1)(f))
• **Data Category:**	Device Data.

• **Optional or Mandatory:**	Optional.

3.6 Management of Social Media Accounts

When you interact with our social media accounts by reacting to posts, sending messages, or following our pages, we will process the following data.

• **Lawful Basis:**	Consent (GDPR Article 6(1)(a))
• **Data Category:**	Social Media Interaction Data.
• **Optional or Mandatory:**	Optional.

3.7 Inquiries, Requests, and Complaint Handling

When you contact us with an inquiry, request, or complaint, we process the following data.

• **Lawful Basis:**	Consent (GDPR Article 6(1)(a))
• **Data Category:**	Identity Data; Your Account and Contact Data; Inquiry, Request, or Complaint Data.
• **Optional or Mandatory:**	Optional.

3.8 Fulfilling Legal Obligations and Protecting Our Legal Interests

If you have a contract with us, we keep your data for the required time to protect our legal rights if needed. Some data must also be kept to follow legal rules on accounting and record-keeping. If you are involved in a legal case with us, we will use this data as needed for that process.

• **Lawful Basis:**	Legal Obligation (GDPR Article 6(1)(c)) and Legitimate Interest in Protecting Our Rights and Legal Interests (GDPR Article 6(1)(f))
• **Data Category:**	Identity Data; Inquiry, Request, or Complaint Data; Legal Data other relevant data.
• **Optional or Mandatory:**	Optional.

4 How do you obtain my Data?

Most of the Data we collect comes directly from you. However, for certain purposes, we may also obtain data from other sources, such as:

Source of Data:	**Purpose of Data Processing**
• Public state registers; • Lists of politically exposed persons (PEPs) and sanctioned individuals; • Legal entities, when you act as their representative, employee, founder, shareholder, participant, beneficiary, governing body member, or hold a similar role; • Our customers, when they provide your data as a spouse, family member, or relative.	Identity verification; enforcement of AML/CTF measures and international sanctions
• Financial institutions, such as: credit institutions, payment service providers and organizations facilitating provision of payment services.	Payment processing; enforcement of AML/CTF measures and international sanctions

• From courts or other government authorities, when we are involved in legal proceedings related to you or required to fulfil legal obligations.	Compliance with legal requirements and the protection of our legal interests.
• Social media service providers.	Administration of social media accounts.

5 Duration of Data Retention

The period for which we retain your Data depends on the purpose of the processing and our role, whether as a data controller or as a data processor acting on behalf of Quicko.

5.1 Where we act as a data processor (processing Data on behalf of Quicko)

Where we process Data on behalf of Quicko in relation to payment services (e.g., Identity Data, Financial Transaction Data, Data concerning implementation of AML/CTF and International Sanctions measures), retention periods are determined by Quicko in accordance with its legal obligations. For more information on data retention for these purposes, please refer to Quicko's Privacy Policy, which you can access **here**.

5.2 Where we act as a data controller

Where we process your Data for our own purposes as data controller, we retain it for the following durations:

Purpose (and Data categories processed within this purpose as set out in Section 3 above):	**Retention Period**
Marketing, promotions	Until you withdraw consent or object.
Social media management	Until you withdraw your consent or delete your social media interaction (such as by removing posts, unfollowing our account, or otherwise deleting the interaction).
Mobile Application account management, customer behavior and analytics	While your account is active and for up to 3 years after closure or inactivity, unless a longer retention period is required to comply with our legal obligations or resolve disputes.
Inquiries, request and complaints	Until resolved and up to 3 years thereafter.
Data necessary for protecting our legal interests	Up to 10 years, in line with the general limitation period for claims under applicable civil laws.

6 Sharing of your Data

When required for the purposes outlined in this Policy above and in accordance with applicable laws, we share data with the following recipients:

- **Nova group companies**: We share Data within the NOVA group of companies (such as: NovaPay LLC (Ukraine), NovaPay Solutions LCC (Ukraine), and other companies belonging to the NOVA Group) to deliver the best possible service, enhance existing offerings, develop new services, develop and improve our EEA / UA Mobile Application, to provide relevant updates about our services, and carry out other necessary activities as outlined above.
- **Quicko Sp. z o.o.**: provider of payment services. NovaPay, as a partner of Quicko, provides the Quicko Mobile Application, which allows users to access Quicko services.
- **Ondato UAB**: identity verification service provider. In order to use the services, we need to perform identity verification process, where biometric data of your face and data from your document will be captured through camera and processed. UAB "Ondato" stores the Data for no longer than it is obliged by NovaPay.

You can always submit request regarding your Data for more detailed information at support@ondato.com or NovaPay as outlined in this Policy.

- **InfoBip LLC**: One time password delivery service provider.
- **IT vendors including cloud storage providers**: Hosting and IT services; IT vendors including cloud storage providers to securely store your Data.
- **Banking, payment, and transaction service providers**: Legal entities and organizations facilitating payment transactions and other payment services.
- **Government, law enforcement and tax authorities, and regulatory authorities**: When we are required to comply with a legal obligation, we may share your data with the authorities mentioned above. This includes situations such as detecting fraud, where we must adhere to applicable disclosure laws.
- **Potential or actual business acquirers, including their authorized advisors or representatives**.

Transferring your data outside the EEA

When transferring data outside the EEA, we rely on a European Commission (**EC**) decision confirming that the recipient country, territory, specific sectors within that country, or an international organization provides an adequate level of data protection.

If no such decision exists, your Data may be transferred to a third country or international organization if appropriate safeguards are in place, such as EC-approved Standard Contractual Clauses (**SCCs**) (Article 46(2)(c) of GDPR).

In particular, when you initiate a payment transaction for cash payout in Ukraine, your Data – including Identity Data (such as your first name, last name, date of birth, and nationality), Financial Transaction Data (such as the amount in account and payout currencies, exchange rate, and payout location), and Contact Data (such as your address and phone number) – will be transferred to NovaPay LLC, a licensed payment service provider in Ukraine, to process and execute your payment instruction. This transfer is essential to ensure that the recipient can collect the funds as requested.

Where such transfers occur, they are safeguarded by appropriate measures to ensure that your Data remains protected in line with applicable data protection laws. Specifically, SCCs approved by the EC (pursuant to Article 46(2)(c) of GDPR) are used, which contractually require the recipient to protect your Data to a standard equivalent to that within the EEA.

Please note that the payment services, including payment transactions for sending funds to Ukraine, are provided by Quicko, acting as your payment service provider. You can learn more about how Quicko processes your Data in its Privacy Policy, available **here**.

You may request further information about the safeguards that are applied to transfers of Data outside the EEA, including how to obtain a copy of the applicable SCCs, by contacting us (please refer to **Section 10 "Contact"** below).

In rare cases where an adequacy decision or appropriate safeguards are not available, your Data will only be transferred relying on the limited derogations provided for under Article 49 of GDPR, and where applicable, we will seek your explicit consent separately at the time of transfer.

Please note: You may withdraw your explicit consent to such transfers at any time by contacting us at cc@novapay.lt . Upon withdrawal, we will stop any future transfers of your Data to third countries without an adequacy decision or appropriate safeguards, unless another legal basis applies. This will not affect the lawfulness of any transfer carried out prior to your withdrawal.

7 Your rights regarding Data processing

Subject to the conditions, restrictions, and exceptions set by applicable laws, you have the following rights:

- **Right to Access Data**: The right to receive confirmation from us on whether your data is being processed, and if so, the right to access your data and information about its processing.
- **Right to Rectify Data**: The right to request that we correct any inaccurate Data related to you.
- **Right to be Forgotten**: Right to request to us to erase your Data, when:
  - data is no longer necessary for the purposes for which it was collected or otherwise processed;
  - you withdraw consent, and there is no other legal basis for processing the data;
  - you object to the processing of the data, and there are no overriding legitimate reasons to process it, or when you object to data processing for direct marketing purposes;
  - data has been processed unlawfully;
  - data must be erased to comply with a legal obligation;
  - data was collected for the provision of information society services based on consent.
- **Right to restrict processing**, when:
  - you dispute the accuracy of the data;
  - processing of Data is unlawful, and you do not agree to the data being deleted, requesting instead to restrict its use;
  - we no longer need the data for the intended purposes, but you need it for legal claims, exercise, or defense;
  - you object to the processing of the data, pending verification of whether our legitimate interests outweigh yours.
- **Right to data portability**: When you seek to obtain your provided Data or transfer it to another Data controller, and the Data processing is based on consent or a contract and carried out by automated means.
- **Right to object**: When we collect and use your Data based on a task carried out in the public interest, the exercise of public authority, our legitimate interests, or for direct marketing purposes. If your Data is processed for direct marketing purposes, you have the right to object at any time, and we will immediately stop processing your data for such purposes.
- **Right to withdraw consent**: When Data processing is based on consent, and you wish to withdraw it at any time, without affecting the lawfulness of the processing based on consent before its withdrawal.
- **Right to lodge a complaint**: The right to file a complaint with a supervisory authority if you believe your Data has been processed in violation of the Data protection laws. However, we recommend first contacting us, and we will try to resolve any concerns or requests you may have.

Please note that we have the right to refuse to process your request for the exercise of data subject rights if it is manifestly unfounded or disproportionate, in particular due to its repetitive nature, as well as in other cases provided for by Data protection legislation.

8 Do you make automated decisions about me?

We use profiling for marketing purposes, such as sending personalized notifications (push, SMS, email, etc.) and reminding users of features they haven't used yet. However, we do not make decisions based solely

on automated data processing that would result in legal consequences for you or otherwise significantly affect you in a similar manner.

As explained in Section 3.5, our profiling is limited to improving communication and engagement and does not produce any significant effects on you.

9 Cookies and similar technologies

Website

We use cookies and similar technologies on our Website to ensure its proper functioning, improve your browsing experience, analyze traffic, and provide personalized content and advertisements.

Below is a list of the cookies and tools we use, including their purpose, expiry period and classification:

Cookie / Tool	Purpose	Expiry	Category
Google Ads	Helps evaluate the performance of advertising campaigns by tracking how many users click on our website after clicking a specific ad, along with basic demographic insights about those users.	24 months	Non-Essential (Marketing)
Google Analytics	Set by Google Analytics, these cookies track visitors, sessions, and campaign performance. It helps us understand how users interact with our website by collecting anonymous data and assigning a randomly generated ID to each visitor.	26 months	Non-Essential (Analytics)
AppsFlyer	Used to create personalized tracking links, this cookie helps us identify which ads users engaged with before visiting our website	12 months	Non-Essential (Marketing/Attribution)
Tiktok Pixel	Used by NovaPay to track, improve, and build custom audiences for ads shown on TikTok.	13 months	Non-Essential (Marketing)
Meta Pixel	Used by NovaPay to track, optimize, and create audiences for advertising campaigns across Meta platforms.	3 months	Non-Essential (Marketing)
Cookiebot	A scanner that checks our website monthly to identify the cookies and tracking technologies in use.	12 months	Essential (Compliance)

Some cookies and tracking tools used on our Website are classified as “non-essential” and require your prior consent under applicable data protection laws. You can manage or withdraw your consent to non-essential cookies and tracking tools at any time via our Cookie Management Platform, powered by Cookiebot.

Mobile Application

We do not use cookies in the traditional web sense in our **Mobile Application**. However, we do use similar technologies to ensure the proper functioning of the Mobile Application, understand user behavior, improve user experience, and send personalized content or notifications.

Below is a list of the technologies we use, including their purpose and expiry period:

Technology	Purpose	Expiry
Google Firebase Analytics	To measure user engagement and behavior within the app	6 months https://firebase.google.com/support/privacy
Push notification identificators	To deliver push notifications	Until the app is uninstalled or the user disables push notifications
AppsFlyer	To attribute installs and in-app events, and measure advertising performance	up to 24 months https://www.appsflyer.com/legal/services-privacy-policy/

These technologies help us better understand how users interact with the Mobile Application and tailor our communication and improvements accordingly.

10 Contact

You can reach our Data Protection Officers, as well as submit a request or lodge a complaint, via email at:

- **NovaPay EU UAB DPO**: dpo@novapay.lt

We will respond within 1 month. If needed, this period may be extended by up to 2 additional months, depending on the complexity of the request, the volume of processed data, and the number of services provided.

You also have the right to lodge a complaint with the Lithuanian State Data Protection Inspectorate.