

OpenApp Pay Privacy Policy

valid from 10/08/2026

openapp

1. Introduction

OpenApp Pay Sp. z o.o., with its registered office in Warsaw at ul. Grzybowska 62, 00-844 Warsaw (hereinafter referred to as OpenApp), takes special care in the area of protection of the personal data of its Users.

This Privacy Policy is a supplement to the OpenApp Application Terms and Conditions and describes the principles of personal data processing in connection with the use of the Application, including purchasing, payment, recommendation and social media functions.

If you have any questions, you can contact us by email: rodo@open-app.com or by sending a letter to our correspondence address: OpenApp Pay Sp. z o.o., ul. Grzybowska 62, 00-844 Warsaw.

The OpenApp Privacy Policy does not regulate the privacy policies of our Partners (e.g. online stores), which are separate data controllers.

We encourage you to review each Partner's privacy policy before entering into a purchase agreement with them. It is available on their website and visible when using the Order and Pay service in the OpenApp application.

OpenApp provides Partners only with the data necessary to complete the order, in accordance with the Application Regulations.

If you do not agree to this Privacy Policy, please do not install or uninstall the Application.

2. Data administrator

The administrator of your personal data is:

OpenApp Pay sp. z o.o.
Grzybowska Street 62
00-844 Warsaw

3. Use of personal data by OpenApp.

We use personal data to verify your identity, provide the Services, communicate with you, ensure security, prevent fraud and comply with the law, present products, make recommendations, and enable you to use the social features available in the Application.

Below you will find a complete summary of the data we collect, the purpose of its processing, the legal basis and the retention period.

Providing personal data is mandatory to the extent necessary to conclude and implement the Agreement and to comply with legal obligations.

Within the remaining scope, providing data is voluntary, but it may be necessary to use certain features of the Application (e.g., social functions, recommendations, or access to contacts).

	Purpose of processing, scope of data processing	Legal basis	Processing time
1.	Registering an account in the Application username, age, phone number, email address and information about your mobile device (e.g. device manufacturer, phone model, operating system version)	Article 6, paragraph 1, letter b of the GDPR – Application Regulations Article 6 section 1 letter c of the GDPR in connection with, among others, Article 75 of the Payment Services Act and, among others, Article 33 et seq., Article 49 of the Act on Counteracting Money Laundering and Terrorist Financing Article 6 paragraph 1 letter f of the GDPR – the legitimate interest of the controller, which we consider to be the processing of data for the purpose of establishing a defence and pursuing claims	If you do not complete Registration, we process your data for 3 days. If you complete the Registration, we process your data for the entire duration of the Agreement until the termination or expiration of the Agreement, and then until the expiry of the limitation period for any claims arising from the Agreement - currently for a period of 6 years counted from the termination or expiration of the agreement for the provision of payment services, with the end of the period always falling on the last day of the year.
2.	Image A photo that can be added at any time while using the Application	Article 6(1)(a) of the GDPR – consent to data processing	We process your consent for the duration of its validity, i.e., until you withdraw it, which we consider, among other things, to be deleting the photo from your account in the Application.
3.	User identification and identity verification First name, last name, PESEL number or date of birth, citizenship, ID card number and series, ID card expiry date, PEP status, ID card photo, and selfie. In the case of verification using the mObywatel method, we may also process the data provided through this method: maiden name, father's name, mother's name, mother's maiden name, country of birth, gender, registered address, registered date, and the authority issuing the ID card.	Article 6 paragraph 1 letter c of the GDPR in connection with, among others, Article 33 et seq., Article 49 of the Act on Counteracting Money Laundering and Terrorist Financing, among others, Article 75 of the Act on Payment Services, Article 6(1)(f) of the GDPR - the legitimate interest of the controller, which we consider to be the processing of data for the purpose of establishing, defending and pursuing claims	We process data for the entire duration of the Agreement from the date of verification until the termination or expiration of the Agreement, and then until the expiry of the limitation period for any claims arising from the Agreement - currently for a period of 6 years counted from the termination or expiration of the agreement for the provision of payment services, with the end of the period always falling on the last day of the year.

4.	Service Implementation Depending on the Service and the details of its implementation, the following data are required: name, phone number, delivery address, location, IP address, mobile device type. In the case of invoice data, additionally: company name, business address, Tax Identification Number (if you are a sole proprietorship)	Art. 6 sec. 1 letter b GDPR – performance of the User Agreement regarding the use of functions available in the Application Article 6 paragraph 1 letter f of the GDPR – the legitimate interest of the controller consisting in the technical processing of the order in the Application, providing the Partner with the data necessary to fulfil the order, and establishing, defending, and pursuing claims. Article 6 paragraph 1 letter a of the GDPR – the User's consent regarding location data, if the use of a given function requires access to location.	We process data for the entire duration of the Agreement, and then until the expiry of the limitation period for any claims arising from the Agreement - currently for a period of 6 years counted from the termination or expiration of the agreement for the provision of payment services, with the end of the period always falling on the last day of the year. We process location data from the date you consent to the processing of location data until you withdraw your consent, which we consider to be the exclusion of sharing your location with us at the mobile phone level.
5.	User Profile Username, age, telephone number, email address, delivery addresses, payment card type and partially masked number, In the case of invoice data, additionally: company name, business address, Tax Identification Number (if you are a sole proprietorship)	Article 6, paragraph 1, letter b of the GDPR – Application Regulations Article 6 section 1 letter c of the GDPR in connection with, among others, Article 75 of the Payment Services Act and, among others, Article 33 et seq., Article 49 of the Act on Counteracting Money Laundering and Terrorist Financing Article 6 paragraph 1 letter f of the GDPR – the legitimate interest of the controller, which we consider to be the processing of data for the purpose of establishing a defence and pursuing claims	We process data for the entire duration of the Agreement, and then until the expiry of the limitation period for any claims arising from the Agreement - currently for a period of 6 years counted from the termination or expiration of the Agreement for the provision of payment services, with the end of the period always falling on the last day of the year.
6.	Consideration of complaints regarding the use of OpenApp Services Data you provide to us, e.g. name and surname, e-mail address or phone number, content of the application, data regarding Payments or operation of the Application.	Article 6 paragraph 1 letter b of the GDPR – performance of the Agreement, Article 6 paragraph 1 letter c of the GDPR – obligations arising from the provisions on payment services and complaint handling by financial market entities, Article 6 paragraph 1 letter f of the GDPR – legitimate	We process data throughout the complaint processing period and for the period required by law, or until the expiry of the limitation period for claims.

		interest of the controller consisting in documenting complaints and in the establishment, defence and pursuit of claims.	
7.	Correct operation of the OpenApp Application Technical data and information necessary to ensure proper operation of the Application, security, error diagnosis and service stability.	Article 6 paragraph 1 letter f of the GDPR - the legitimate interest of the controller, which is considered to be, among others, the need to maintain the proper functioning of the Application	Data processed throughout the period of use of the Application or until an objection to data processing is filed
8.	Usage data by the Application User, including data relating to launching the Application, navigating it, and performing individual actions within the scope of data related to a given account.	Article 6(1)(f) of the GDPR - the legitimate interest of the controller, which we consider to be the need to enable OpenApp to make corrections	Data processed throughout the period of use of the Application or until an objection to data processing is filed
9.	Product and basket recommendations Data regarding your purchase history, purchase frequency, purchase activity in the Application and purchase preferences, including activity in various stores available in the Application.	Article 6, paragraph 1, letter f of the GDPR – the legitimate interest of the controller in personalising the content presented in the Application, including matching product recommendations and shopping carts to the User's preferences and improving the operation of the Application	Data processed throughout the period of use of the Application or until an objection to data processing is filed
10.	Creating a Personal Store Data on products purchased, products saved, liked, added to cart, recommended and other interactions of the User with products in the Application	Article 6, paragraph 1, letter f of the GDPR – the legitimate interest of the controller in presenting the User with products related to their activity in the Application, including creating a Personal Store, and improving the use of the Application	Data processed throughout the period of use of the Application or until an objection to data processing is filed
11.	Social features Data about User activity and interactions, including information about invitations, shared carts, scope of permissions in shared carts, following Personal Stores, and information visible to other	Article 6(1)(b) of the GDPR – processing necessary to provide services within the Application, in particular to enable the use of social media functions.	Data processed for the period of use of the social functions available in the Application, and then for the limitation period for any claims.

	Users in accordance with privacy settings.		
12.	Invitations and use of contacts Telephone number and other contact details of the selected person from the User's contacts.	Article 6, paragraph 1, letter a of the GDPR – the User's consent to access contacts stored on the device and to use selected contact data for the purpose of sending invitations to use the Application or its functionalities.	Data processed until the invitation is sent or the User withdraws consent.
13.	Data provided in connection with the recording of calls made by the Customer Service Office	Article 6 paragraph 1 letter f of the GDPR – the legitimate interest of the controller, which we consider to be the need to record telephone conversations in the event of proving facts and evidence	We process the data for a period of 3 months from the date of the conversation

4. Who do we share or transfer data to?

We want to assure you that we do not transfer your data to other entities without a legitimate reason and legal basis.

Below, we indicate situations in which we may share data with controllers other than us who are recipients of personal data. These include:

- **Partners**- to the extent necessary to complete the order and in accordance with the Application Regulations.
- **State bodies and institutions**: entities or persons authorised under the provisions of law to process personal data for the purposes of proceedings conducted by them or in order to fulfil OpenApp's obligations arising from the provisions of law, e.g. the Polish Financial Supervision Authority, the Chief Inspector of Financial Information;
- banks, credit institutions, payment institutions, settlement agents other than OpenApp, entities operating a payment system or payment scheme, electronic money institutions, financial institutions providing funds transfer services, telecommunications operators for the purpose of resolving potential Complaints with them;
- law firms;
- other users of the App, to the extent necessary to use the App's social features, in particular shared baskets, invitations, and the Personal Store. The scope of information visible to other users within social features, including the Personal Store, depends on the privacy settings in the App and the actions the User takes.

We may entrust personal data to external entities under a data processing agreement, in particular to OpenApp sp. z o.o., a company belonging to the same

capital group. In such cases, the data is processed only in accordance with our instructions by **OpenApp service providers** providing us with services in the field of customer service, accounting services, remote identity verification, IT services providers, technical and technological solutions, e-mail and IT system providers, companies providing consultancy services in the field of personal data protection, auditing companies, providers of solutions related to the lease of space in which the OpenApp office is located

We do not sell your personal data or share it with third parties for marketing purposes.

5. How do we obtain personal data?

We obtain personal data directly from Users, from their activity in the Application, as well as from banks - each time with the consent of Users expressed to the bank - and, if such a verification method is chosen, via the mObywatel application, as part of the identity verification process required by law to ensure financial security.

6. What device resources does the OpenApp application have access to?

After the User's consent, the Application has access to:

- Phone name information;
- Information about the location of your mobile device when using the Services
- Selected contacts when using selected functionalities of the Application;
- Camera when you scan a QR code and take a photo of your ID or selfie as part of your chosen identity verification method; we do not have access to photos or videos stored on your device.

7. How do I block access to device resources for OpenApp applications?

Application permissions may be revoked at any time by changing the system settings on your mobile device or by uninstalling the Application.

8. What notifications and messages do we send in the app?

We may send App Users push notifications or messages if the User consents (Article 6, Section 1, Letter a of the GDPR). By default, notifications are disabled; however, it is recommended to enable them for the User's convenience and increased security. Consent may be withdrawn at any time through the mobile device's system settings.

Withdrawing consent does not affect the lawfulness of processing based on consent before its withdrawal. We process data to improve the use of the Application for the duration of the consent's validity until its withdrawal.

We may also send messages displayed directly in the Application, which cannot be disabled (e.g. regarding changes to the Terms and Conditions, technical

information, order fulfillment status) – we process data in connection with messages based on the legitimate interest of the controller under Article 6 paragraph 1 letter f of the GDPR in order to inform the User about necessary changes, provide important information for the duration of the controller's legitimate interest or until an objection to data processing is filed.

We do not send any e-mail or SMS messages to Users requesting any personal data – in particular login details or any information concerning the User.

9. What rights do you have regarding personal data protection in OpenApp?

You have the right to access, rectify, erase, transfer, and restrict the processing of your data, as well as the right to withdraw consent at any time. Withdrawing consent does not affect the lawfulness of processing based on consent before its withdrawal. The data subject is informed of this before giving consent.

You have the right to object to the processing of your personal data at any time when we process it based on the controller's legitimate interest.

To exercise your rights, please write to us at the correspondence address or e-mail address provided in point 1 above.

You also have the right to lodge a complaint with a supervisory authority. In Poland, this is the President of the Personal Data Protection Office: correspondence address: Personal Data Protection Office, ul. Stawki 2, 00-193 Warsaw, kancelaria@uodo.gov.pl, Hotline: 606-950-000.

10. Is your personal data transferred between countries?

Personal data will generally not be transferred outside the European Economic Area (hereinafter referred to as the "EEA"). Given the provision of services by our subcontractors in support of ICT services and IT infrastructure, we may outsource certain IT activities or tasks to recognised subcontractors operating outside the EEA, which may result in the transfer of your data outside the EEA.

Personal data may be transferred to countries for which the European Commission has not issued an adequacy decision. In such situations, we use the tools specified in Article 46(2)(c) of the GDPR (so-called standard contractual clauses) or transfer data based on other legal bases for data transfer specified in Article 49 of the GDPR. The method of securing your data in these cases complies with the principles set out in Chapter V of the GDPR. You can request further information about the safeguards applied in this regard at any time, obtain a copy of these safeguards, and learn where they are shared.

11. Cookies and other tracking technologies.

We do not use cookies in the context of website technologies. However, we may use analytical and diagnostic tools, such as Firebase, to help us analyse the App's performance, detect errors, and improve its functionality.

12. The principle of creating anonymous email addresses

In the Application, when communicating with Partners, we always use an anonymous email address generated uniquely for each User and each Partner. For Partners that are part of a single capital group, the anonymous email address also includes a unique identifier identifying the online store.

13. Do we process personal data for the purposes of automated decision-making, including profiling?

Profiling means the automated use of personal data to evaluate certain factors relating to a natural person, e.g., their preferences, interests, or behaviour.

In the Application, we may use profiling, consisting of the analysis of User activity, in particular purchase history, purchase frequency, products saved, liked, or added to the cart, to present product and cart recommendations, create a Personal Store, and personalise the content presented in the Application.

We do not make decisions about you based solely on automated processing, including profiling, that would produce legal effects for you or significantly affect you in a similar manner.

14. Privacy Policy Changes

The Policy takes effect on the date the App launches and may be updated. You will be notified of each update at least 14 days in advance via an in-app notification about upcoming changes, along with an updated version of the Privacy Policy.