

Privacy and cookie policy
OpenApp Pay website

valid from 16/09/2026

openapp

1. General information

- a. This Privacy and Cookies Policy, hereinafter referred to as the "Policy", describes the principles for processing the personal data of persons using the OpenApp Pay website at www.open-app.com, including people who send messages or complaints via the contact form.
- b. The Policy also contains information regarding the use of cookies and similar technologies on the Website.
- c. This policy applies only to the Website. The privacy policies for the OpenApp Application, the OpenApp Service, and the payment services provided by OpenApp describe the principles of personal data processing in connection with their use.

2. Personal data administrator

- a. The controller of personal data is OpenApp Pay Sp. z o.o. with its registered office in Warsaw, ul. Grzybowska 62, 00-844 Warsaw, entered into the Register of Entrepreneurs of the National Court Register under the KRS number 0000842899, NIP 9512501827, REGON 386124823, hereinafter referred to as "OpenApp" or "Administrator".
- b. In matters concerning the processing of personal data or the exercise of rights related to data processing, you can contact OpenApp:
 - i. by e-mail at: rodo@open-app.com;
 - ii. in writing to the following address: OpenApp Pay Sp. z o.o., ul. Grzybowska 62, 00-844 Warsaw;
 - iii. via the contact form available on the Website.

3. What data do we process?

- a. In connection with the use of the Website, OpenApp may process technical data transmitted by the User's device and browser, in particular:
 - i. IP address;
 - ii. date and time of connection;
 - iii. information about your browser, operating system and device type;
 - iv. information about the resource being called or the occurrence of an error;
 - v. information saved in server logs and security systems.
- b. If you use the contact form, OpenApp processes:
 - i. name and surname;
 - ii. e-mail address;
 - iii. telephone number, if provided;
 - iv. company name, if provided;
 - v. subject and content of the message;

- vi. other data voluntarily included by the User in the message content.
- c. If the message constitutes a complaint regarding the OpenApp Application, the OpenApp Service, or a payment service, OpenApp may also process the data necessary to identify the User, the service, or the payment and to consider the complaint, in particular the payment identifier, its date, amount, and a description of the reported event.
- d. The User should not provide any data that is not necessary to describe the case, in particular payment card details, BLIK codes, passwords, authentication codes, or copies of identity documents.
- e. If the report concerns another person, the User should provide their data only if he or she is authorised to do so or if it is necessary to describe the matter.

4. Purposes and legal basis of processing

- a. OpenApp processes personal data for the following purposes:
 - i. **providing access to and ensuring the proper functioning of the Website**– pursuant to Article 6(1)(b) of the GDPR, to the extent necessary to provide services electronically, and Article 6(1)(f) of the GDPR, on the basis of OpenApp's legitimate interest in ensuring the proper functioning of the Website;
 - ii. **handling questions, opinions and other messages sent via the contact form**– pursuant to Article 6(1)(f) of the GDPR, i.e. OpenApp's legitimate interest in communicating and providing responses;
 - iii. **taking action at the request of a person before concluding a contract**– pursuant to Article 6(1)(b) of the GDPR, if the message concerns the possibility of concluding a contract or starting to use the service;
 - iv. **handling complaints regarding the Website or the contact form**– pursuant to Article 6 paragraph 1 letter b of the GDPR, to the extent necessary to perform the contract for the provision of services by electronic means, and Article 6 paragraph 1 letter c of the GDPR, if the obligation to consider the complaint results from the provisions of law;
 - v. **accepting and considering complaints regarding the OpenApp Application, OpenApp Service or payment service**– pursuant to Article 6(1)(b) of the GDPR, to the extent necessary for the performance of the relevant contract, and Article 6(1)(c) of the GDPR, in order to comply with legal obligations incumbent on OpenApp as a payment service provider or financial market entity;

- vi. **ensuring the security of the Website and contact form, preventing spam, fraud and other abuses, and detecting security incidents**– pursuant to Article 6(1)(f) of the GDPR, i.e. the legitimate interest of OpenApp in protecting the Website, IT systems and data;
 - vii. **keeping aggregate statistics regarding the use of the Website**– pursuant to Article 6(1)(f) of the GDPR, i.e. OpenApp's legitimate interest in analysing the popularity of individual content and improving the operation of the Website;
 - viii. **establishing, investigating or defending against claims**– pursuant to Article 6(1)(f) of the GDPR, i.e. OpenApp's legitimate interest in protecting its rights.
- b. If OpenApp's legitimate interest is the basis for processing, the User may object to the processing on the terms described in point 9 of the Policy.

5. Is providing data mandatory?

- a. Providing data marked as mandatory in the form is voluntary, but necessary to submit the application and receive a response.
- b. Providing your company name and phone number is voluntary. Failure to provide this information will not prevent you from submitting the form.
- c. If the submission constitutes a complaint, you may need to provide certain information to identify the service or payment and process the matter. If the information provided proves insufficient, OpenApp may request additional information.

6. Data recipients

- a. Personal data may be transferred to entities supporting OpenApp in running the Website and handling requests, in particular:
 - i. Amazon Web Services EMEA SARL and entities from the Amazon Web Services group providing hosting, IT infrastructure, security and technical support services;
 - ii. email provider used by OpenApp;
 - iii. providers of IT services, maintenance and security of the Website;
 - iv. Google Ireland Limited and entities from the Google group, in connection with the use of the Google reCAPTCHA mechanism;
 - v. legal advisors, auditors and other professional advisors, if necessary to handle the matter or protect OpenApp's rights;
 - vi. public authorities and other authorised entities, if the obligation to provide data results from legal provisions.
- b. Entities processing data on behalf of OpenApp may process it only in accordance with the contract concluded with OpenApp and OpenApp's

documented instructions, unless the entity processes the data as an independent controller.

7. Transfer of data outside the European Economic Area

- a. OpenApp uses the services of globally operating providers, in particular Amazon Web Services and Google. By using their services, personal data may be accessible to entities located outside the European Economic Area ("EEA").
- b. If personal data are transferred outside the EEA, OpenApp ensures that the appropriate mechanism provided for in the GDPR is applied, in particular:
 - i. a decision of the European Commission establishing an adequate level of data protection – if the recipient is covered by such a decision; or
 - ii. standard contractual clauses approved by the European Commission, together with additional safeguards where required.
- c. You can obtain information about the security measures used by contacting OpenApp at rodo@open-app.com.

8. Data storage period

- a. Data relating to a simple question, opinion, or message is stored for the period necessary to respond and complete the correspondence, and then until the expiry of the limitation period for any claims, if retaining the data is necessary to protect OpenApp's rights.
- b. If the correspondence leads to the conclusion of a contract, we may store the data for the duration of the contract and then for the period required by law and the limitation period for claims.
- c. Data relating to a complaint relating to the Website or the contact form are stored for the period of consideration of the complaint and then until the expiry of the limitation period for claims related to the case.
- d. Data relating to a complaint relating to the OpenApp Application, OpenApp Service or payment service are stored for the period required by the regulations applicable to the given service, including regulations on payment services, anti-money laundering, accounting and complaint handling, and then – if necessary – until the expiry of the limitation period for claims.
- e. The limitation period for claims is, depending on the type of case, generally three or six years, and may end at the end of a calendar year.
- f. Data contained in technical and security logs are retained for the period necessary to ensure the security of the Website, detect incidents and investigate irregularities, but no longer than 12 months, unless longer retention is necessary in connection with a specific incident, proceeding or claim.

- g. Data may be stored longer if legal provisions require it, a competent authority requests it, or it is necessary to establish, pursue, or defend against claims.

9. Data subject rights

The data subject has the right to:

- a. obtaining information on the processing of personal data and access to data,
- b. rectification of incorrect data and supplementation of incomplete data,
- c. deletion of data,
- d. restrictions on data processing,
- e. data portability if processing is based on consent or a contract and is carried out in an automated manner,
- f. object to processing based on the legitimate interest of OpenApp, for reasons related to the particular situation of that person
- g. withdraw consent at any time, if the processing is based on consent, without affecting the lawfulness of processing carried out before its withdrawal.

To exercise your rights, please contact OpenApp at rodo@open-app.com or in writing to the address of OpenApp's registered office.

OpenApp may request additional information if it is necessary to confirm the identity of the person submitting the request.

A person who believes that their data is being processed unlawfully may file a complaint with the President of the Personal Data Protection Office.

10. Google reCAPTCHA

- a. The contact form is secured using Google reCAPTCHA, which is designed to distinguish actions performed by humans from those performed by bots and to protect the form from spam, fraud and other abuses.
- b. In connection with the operation of reCAPTCHA, Google may receive in particular:
 - i. device IP address;
 - ii. information about your browser, operating system and device;
 - iii. date and time of connection;
 - iv. information on how to use the Website and the form, necessary to conduct risk analysis;
 - v. information read or written on the User's device, including through cookies or similar technologies.
- c. We process the data to ensure the security of the Website and the contact form and to prevent abuse. OpenApp processes data on the basis of Article

6(1)(f) of the GDPR, i.e., OpenApp's legitimate interest in protecting the form and IT systems.

- d. reCAPTCHA is provided by Google Ireland Limited. Google may also process data as a separate controller, as set out in its Privacy Policy and Terms of Service.
- e. Disabling the technologies required for reCAPTCHA to function may prevent you from submitting the contact form. In such a case, you may contact OpenApp by email, telephone, or in writing.

11. Cookies and similar technologies

- a. Cookies are small computer files stored on the User's device. The website may also use other technologies to store information on the User's device or access information already stored there.
- b. The website may use technologies necessary to:
 - i. proper display and operation of the Website;
 - ii. ensuring connection security;
 - iii. protecting the contact form against spam and other abuses;
 - iv. maintaining the technical settings necessary for the operation of the Website.
- c. OpenApp independently compiles aggregated statistics regarding Website usage. The tool used for this purpose does not use cookies or other technologies that store information on the User's device, does not create persistent User identifiers, and is not intended to track User activity across different websites.
- d. Google reCAPTCHA may use cookies and similar technologies to ensure form security and evaluate whether a human or an automated system is using the form.
- e. The technologies indicated in point 12(b) and (d) are used only to the extent necessary to provide the service requested by the User or to ensure the security of the Website and the form. OpenApp does not use them to conduct its own behavioural advertising.
- f. The website does not use marketing cookies or OpenApp cookies to track users across different websites.
- g. Users can manage cookies through their browser settings, in particular by blocking their storage or deleting existing cookies. Limiting the use of certain technologies may affect the proper functioning of the contact form.
- h. If, in the future, OpenApp starts using technologies that are not necessary for the operation of the Website or the provision of the service requested by the User, they will only be activated after obtaining the required consent.

12. Automated decision-making and profiling

- a. OpenApp does not use personal data processed in connection with the use of the Website and the contact form to make decisions about the User based solely on automated processing that would produce legal effects for him or her or significantly affect him or her in a similar manner.
- b. reCAPTCHA performs an automated risk assessment to determine whether a form is being used by a human or an automated system. This assessment may affect the ability to submit the form, but does not have any legal effect on the User or significantly affect them.

13. Data security

- a. OpenApp uses appropriate technical and organisational measures to protect personal data against unauthorised access, loss, destruction, alteration or unauthorised disclosure.
- b. The website uses the Amazon Web Services infrastructure.
- c. Access to personal data is limited to those who need it to perform their duties.
- d. The user should not provide confidential information or data via the form that is not necessary to process the case.

14. Policy Changes

- a. The policy may be changed in particular in the event of:
 - i. changes to the operation of the Website or contact form;
 - ii. implementation of new tools or technologies;
 - iii. changes to the scope or purposes of data processing;
 - iv. changes in legal provisions or their interpretation.
- b. The current version of the Policy is published on the Website along with the date it comes into effect.
- c. Changes to the Policy take effect on the date indicated in the new version.