Privacy Policy

This Privacy Policy (hereinafter: "Policy") contains information on the processing of your personal data in connection with the use of Atlas Pickup Points App, (hereinafter: "App").

Any capitalised terms not otherwise defined in the Policy shall have the meaning given to them in the TOS, available at: https://atlaspickuppoints.com/legal/terms.

This Privacy Policy applies to the processing of the Merchant's personal data. The processing of Buyers' personal data is governed by a separate data processing agreement.

Controller

The Controller of your personal data is Patryk Jakubik, running a business under the name PATRYK JAKUBIK with its registered office in Zielonka, at Prymasa Stefana Wyszyńskiego 7H/4, 05-220 Zielonka, Poland, entered into the Central Register of Information on Business Activity kept by the minister competent for the economy, having NIP (TIN): 8672245025, EU VAT number: PL8672245025, REGON: 380109870 (hereinafter: "Controller").

Contact with the Controller

In all matters related to the processing of personal data, you can contact the Controller via email – at: privacy@atlaspickuppoints.com.

Personal data protection measures

The Controller applies modern organisational and technical safeguards to ensure the best possible protection of your personal data and guarantees that it processes them in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter: "GDPR"), the Act of 10 May 2018 on the Protection of Personal Data and other Personal Data Protection Regulations.

In particular:

1. the App and its databases are hosted in data centres located within the European Union;
2. all data transmitted between your device, the App and the Controller's infrastructure is encrypted in transit using TLS;
3. access to personal data is limited to the persons for whom it is necessary in order to provide the Service, is granted individually and is subject to authentication;
4. the Controller entrusts the processing of personal data only to the entities included in the subprocessor list referred to in the section on recipients of personal data, on the basis of the agreements referred to in that section.

Information on the personal data processed

The use of the App requires the processing of your personal data. Below you will find detailed information about the purposes and legal grounds of processing, as well as the period of processing and the obligation or voluntariness to provide them.

Purpose of processing	Personal data processed	Legal basis
Conclusion and performance of the Service Agreement (App)	name and surname of the store owner and of the persons using the App on the Merchant's behalf email address telephone number business name, store name and Shopify store address store identifier, country and currency selected plan, subscription period and billing details of the subscription interface language other information provided by the Merchant	Article 6(1)(b) of the GDPR (processing is necessary for the performance of the Service Agreement concluded with the data subject or to take steps to conclude it)
Providing the above-mentioned personal data is a condition for concluding and performing the Service Agreement (providing them is voluntary, but the consequence of failure to provide them will be the inability to conclude and perform the Service Agreement). The Controller will process the above-mentioned personal data until the statute of limitations for claims arising from the Service Agreement expires.		

Purpose of processing	Personal data processed	Legal basis
Conducting a complaint procedure	name and surname business name/store name email address other data provided by Merchant via complaint	Article 6(1)(b) of the GDPR (processing is necessary for the performance of the Service Agreement and for the Merchant to exercise the rights granted to them under the Agreement)
Providing the above-mentioned personal data is a prerequisite for receiving a response to a complaint or for the Merchant to exercise their rights under the Agreement (providing this data is voluntary; however, failure to do so will result in the inability to receive a response to the complaint or to exercise the aforementioned rights). The Controller will process the above-mentioned personal data for the duration of the complaint proceedings, and in the case of exercising the Merchant's aforementioned rights – until such rights expire.		

Purpose of processing	Personal data processed	Legal basis
Conducting a verification procedure and considering appeals against decisions on dealing with unacceptable content	name and surname/business name, contact details, including email address	Article 6(1)(c) of the GDPR (processing is necessary for compliance with a legal obligation to which the Controller is subject, in this case the following obligations: provide a mechanism for reporting inappropriate content (Article 16 of Regulation 2022/2065 on the single market for digital services and amending Directive 2000/31/EC (Digital Services Act) (hereinafter: "DSA") handling appeals (Article 20 of the DSA).
Providing the above-mentioned personal data is a condition for receiving a response to the report or exercising the Merchant's rights under the provisions of the DSA (their provision is voluntary, but the consequence of failure to provide them will be the inability to receive a response to the report and the exercise of the above-mentioned rights). The Controller will process the above-mentioned personal data for the duration of the procedure, and in the case of exercising the above-mentioned rights of the Merchant – until their limitation expires.		

Purpose of processing	Personal data processed	Legal basis
Handling queries submitted by Merchants	name email address other data contained in the message to the Controller	Article 6(1)(f) of the GDPR (processing is necessary for the purpose of pursuing the legitimate interest of the Controller, in this case responding to the inquiry received)
Providing the above-mentioned personal data is voluntary, but necessary in order to receive a response to the inquiry (the consequence of failure to provide them will be the inability to receive an answer). The Controller will process the above-mentioned personal data until an effective objection is raised or the purpose of processing is achieved (whichever occurs first).		

Purpose of processing	Personal data processed	Legal basis
Compliance with obligations related to the protection of personal data	name and surname contact details provided by you (email address; correspondence address; telephone number)	Article 6(1)(c) of the GDPR (processing is necessary to comply with a legal obligation to which the Controller is subject, in this case the obligations resulting from the provisions on the protection of personal data)
Providing the above-mentioned personal data is voluntary, but necessary for the proper performance by the Controller of the obligations resulting from the provisions on the protection of personal data, e.g. the exercise of the rights granted to you by the GDPR (the consequence of failure to provide the above-mentioned data will be the inability to properly exercise the above-mentioned rights). The Controller will process the above-mentioned personal data until the expiry of the limitation periods for claims for violation of personal data protection regulations.		

Purpose of processing	Personal data processed	Legal basis
Establishing, exercising or defending against legal claims	name and surname/company email address address of residence/registered office TIN	Article 6(1)(f) of the GDPR (processing is necessary for the purpose of pursuing the legitimate interest of the Controller, in this case establishing, investigating or defending against claims that may arise in connection with the performance of the Agreements concluded with the Controller)
Providing the above-mentioned personal data is voluntary, but necessary in order to establish, pursue or defend against claims that may arise in connection with the performance of the Agreements concluded with the Controller (the consequence of failure to provide the above-mentioned data will be the inability of the Controller to take the above-mentioned actions) The Controller will process the above-mentioned personal data until the expiry of the limitation periods for claims that may arise in connection with the performance of the Agreements concluded with the Controller.		

Purpose of processing	Personal data processed	Legal basis
App administration, security and error diagnosis	IP address server date and time web browser and device information operating system information identifier of the store and of the person using the App information about the operation performed and about any error that occurred recording of the session in the App's administration interface captured when an error occurs, with the content of form fields masked The above data are saved automatically in server logs, and – when an error occurs – in error reports and error-triggered session recordings (it would not be possible to administer the App and diagnose technical errors without automatic logging and error reporting).	Article 6(1)(f) of the GDPR (processing is necessary for the purpose of pursuing the legitimate interest of the Controller, in this case ensuring the proper operation and security)
Providing the above-mentioned personal data is voluntary, but necessary to ensure the proper operation of the App (the consequence of failure to provide them will be the inability to ensure the proper operation of the App). The Controller will process the above-mentioned personal data for a period of 30 days, or until an effective objection is raised if this occurs earlier.		

Recipients of personal data

The recipients of personal data are the external entities cooperating with the Controller that are listed at https://atlaspickuppoints.com/legal/subprocessors, together with the service each of them provides, the place where it processes personal data and the basis for any transfer outside the European Economic Area. That list forms part of this Policy, and the Controller updates it whenever the entities it uses change.

In addition, personal data may also be transferred to public or private entities, if such an obligation results from generally applicable law, a final court judgment or a final administrative decision.

Transfer of personal data to a third country

In connection with the Controller's use of the services of the recipients referred to above whose place of processing is outside the European Economic Area, your personal data may be transferred to the United States. The basis for the transfer of data to the above-mentioned third countries are:

- in the case of DPF-certified entities – a decision of the European Commission stating an adequate level of protection of personal data in the relevant third country (the EU-U.S. Data Privacy Framework);
- in the case of non-DPF-certified entities – standard contractual clauses in line with Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries under Regulation (EU) 2016/679 of the European Parliament and of the Council, together with a relevant transfer impact assessment (TIA).

The basis applicable to each recipient is indicated in the list of recipients referred to above.

You can obtain from the Controller a copy of the data transferred to a third country.

Data subject rights

In connection with the processing of personal data, you have the following rights:

1. the right to be informed what personal data concerning you is processed by the Controller and to receive a copy of this data (the so-called right of access). Issuing the first copy of the data is free of charge, for subsequent copies the Controller may charge a fee;
2. if the processed data becomes outdated or incomplete (or otherwise incorrect), you have the right to request its rectification;
3. in certain situations, you can ask the Controller to delete your personal data, e.g. when:
   a) the data will no longer be needed by the Controller for the purposes of which it has informed;
   b) you have effectively withdrawn your consent to the processing of data – unless the Controller has the right to process the data on another legal basis;
   c) the processing is unlawful;
   d) the need to delete the data results from a legal obligation to which the Controller is subject;
4. if personal data is processed by the Controller on the basis of the consent granted to the processing or in order to perform the Agreement concluded with him, you have the right to transfer your data to another Controller;
5. if personal data is processed by the Controller on the basis of your consent to the processing, you have the right to withdraw this consent at any time (the withdrawal of consent does not affect the lawfulness of the processing that was carried out on the basis of consent before its withdrawal);
6. if you believe that the processed personal data are incorrect, their processing is unlawful, or the Controller no longer needs certain data, you can request that for a specified period of time (e.g. checking the correctness of the data or pursuing claims) the Controller does not perform any operations on the data, but only stores them;
7. you have the right to object to the processing of personal data based on the legitimate interest of the Controller. In the event of an effective objection, the Controller will cease to process personal data for the above-mentioned purpose;
8. you have the right to lodge a complaint with the President of the Office for Personal Data Protection if you believe that the processing of personal data violates the provisions of the GDPR.

Cookies and other technologies

1. The App does not install cookies on your end device and does not use cookies of its own. Access to the App is authorised using session tokens issued by Shopify each time the App is opened in the Shopify administrative console. The App keeps information in your browser only where this is necessary for it to function, for example the interface language you select, stored in local storage, or, when an error occurs in the administration interface, the identifier of the error-triggered session recording, stored in session storage and discarded when you close the tab. The App does not store anything in your browser for tracking, profiling, advertising or analytics purposes.
2. The Controller does not track your activity in the App for marketing or advertising purposes, does not use third-party analytics trackers and does not profile you. Solely for the purpose of diagnosing errors, when an error occurs in the App's administration interface, the Controller captures a recording of the session (error-triggered session replay) with the content of form fields masked; these recordings are processed on the terms described in the section on the personal data processed.
3. The Controller processes technical data to the extent necessary to provide the Service, ensure its security and provide support, on the terms described in the section on the personal data processed. This includes in particular data saved automatically in server logs, in error reports and in error-triggered session recordings.

4. The map displayed in the App is provided by Google Maps under the Merchant's own Google Maps API key. The rules for the use of cookies and similar technologies by Google in this respect result from the agreement concluded between the Merchant and Google.

Changes to the Privacy Policy

1. The Controller may amend this Policy, in particular in the event of a change in the scope of the Controller's business, the commencement, modification or discontinuation of services, technical modifications to the App, or a change in the law requiring the Policy to be adapted.
2. Merchants will be informed about a change to the Policy in the same manner as about a change to the Terms of Service: by publication of the amended Policy on the App website and by email. The provisions of § 13 of the Terms of Service on the right to terminate the Service Agreement within 10 days of receiving that information, and on the consequences of not doing so, apply accordingly.
3. Updating the subprocessor list referred to in the section on recipients of personal data does not constitute a change to this Policy. Changes to that list are made on the terms set out in § 5 of the Entrustment Agreement.

Final provisions

To the extent not regulated by the Policy, the generally applicable provisions on the protection of personal data shall apply.

The policy is effective from 4 November 2026.