Privacy Policy

Previous version, valid until 22 October 2026. This version of the Privacy Policy no longer applies. The current version: Privacy Policy.

Migrantora Ltd (collectively, “Migrun”, “MigRun.tech”, “we”, “us”, or “our”) are committed to protecting and respecting your privacy. This privacy policy (“Privacy Policy”), together with our Terms of Service and any other documents referred to in this Privacy Policy, sets out the basis on which any personally identifiable information (“Personal Data”) we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your Personal Data, the kinds of information we may collect, how we intend to use and share that information, and how you can request access, correction, portability, or deletion of such information (our “Privacy Policy”) in respect of your use of Migrun website (“ the Platform”).

By using the Platform, you are accepting the terms of this Privacy Policy. In the event of a conflict between the terms of this Privacy Policy and the Terms of Service, the Terms of Service will prevail.

Information we may collect from you

We may collect and process the following information about you.
Information you give us. If you decide to register with or use the Platform you will be asked to provide certain information about yourself. You will voluntarily provide us with Personal Data which includes your name, email address and contact details when you:

- Purchase or register to use the Platform.
- Sign up to use the Platform via an integrated service, such as Google.
- Request and receive Customer Support.
- Provide billing and payment information.
- Register for offers or events.
- Post comments on our websites.
- Participate in discussion boards or other social media functions on our website.

Information we collect about you. Each time you use the Platform we may automatically collect the following information:

Technical information that your browser sends whenever you visit a website or your mobile app sends when you are using it. This log data may include your Internet Protocol (IP) address, the address of the web page you visited before using the Platform, your browser type and settings, the date and time of your use of the Platform, information about your browser configuration and plug-ins, language preferences and cookie data.

Information about your visit, including the full Uniform Resource Locators (URL) clickstream to, through and from our website (including date and time); page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page and any phone number used to call our customer service number.

We may also collect non-personally identifiable information (e.g. gender and location) to assist in providing the Platform to you. Non-personally identifiable information by itself cannot be used to identify or contact you.

Processing of Sensitive Personal Data

If you instruct us to do so as part of our providing services to you we may process special categories of personal data such as:

Passport copies and other government-issued identification documents;

Criminal record certificates from the country of your location.

We apply heightened security measures to protect such sensitive data, including:

Encryption in transit (TLS 1.2 or higher) and encryption at rest (AES-256 or equivalent)

Role-based access controls to ensure that only authorised personnel with a business need can access the data

Secure storage in data centres located in EU and, where applicable, the EEA, operated by providers that meet recognised security standards

Audit logging of access to sensitive data to detect unauthorised activity

Retention limits – sensitive documents are retained only for as long as necessary to fulfil the service or meet legal requirements, and are securely deleted thereafter.

We never use sensitive personal data for purposes unrelated to the service you have requested, unless required by law or necessary to provide you a requested service or authorised by your explicit consent.
By submitting your Personal Data and non-personally identifiable information, you consent to the collection, use and transfer of your information in accordance with the terms of this Privacy Policy.

Information we receive from other sources. We may receive information about you if you use any of the other websites we operate or the other services we provide. In this case, we will have informed you when we collected that data that it may be shared internally and combined with data collected via the Platform. We are also working closely with third parties (including, for example, business partners, sub-contractors in technical, consulting, payment and delivery services, advertising networks, analytics providers, search information providers, credit reference agencies) and may receive information about you from them.

Testimonials and Success Stories

From time to time, we may invite some of our users to share their real experience with Migrun in the form of a written, audio, or video testimonial. Participation is entirely voluntary. If you agree to provide a testimonial, we will ask for your separate consent to record and publish your name, image, voice and story for promotional purposes (including on our website, social media or marketing materials). You may withdraw your consent at any time by contacting us at privacy@migrun.tech, in which case we will cease using your testimonial in future materials. However, content already published or shared by third parties may not always be fully removable.

Use of Cookies

Cookies and Similar Technologies
We use cookies, pixels, and similar tracking technologies to provide and improve our services, remember your preferences, and deliver relevant services.

We distinguish between:

- Strictly necessary cookies – essential for the website to function and that cannot be disabled.
- Non-essential cookies – including performance, functionality, and targeting/advertising cookies, which are only used with your consent or where required by law.

If you choose so you are allowed to:

- Accept all non-essential cookies
- Reject all non-essential cookies
- Customise your cookie preferences by category

You can change or withdraw your consent at any time through email privacy@migrun.tech.
We use cookies on our website to distinguish you from other users of our website and Service. This helps us to provide you with a good experience when you browse our website and also allows us to improve the website and Service.

If You are Under 18 years of Age

If you're under the age of 18, you may not have an account on the Platform. We do not knowingly collect information from or direct any of our content specifically to children under 18. If we learn or have reason to suspect that you are a user who is under the age of 18, we will, unfortunately, have to close your account. Please see our Terms of Service for information about account termination.

Lawful Bases for Processing

We have a lawful basis for each purpose for which we process personal data and we do not collect excessive data. For your convenience the table below summarises the main purposes for which we process personal data, the categories of data involved, and the corresponding lawful basis.

Purpose of Processing	Categories of Personal Data	Lawful Basis
		Performance of a contract

Account creation and management	Name, contact details, account credentials	
Provision of services (including visa application support)	Identity documents, contact details, supporting documents	Performance of a contract
Payment processing	Billing address, payment details	Performance of a contract / Legal obligation
Customer support	Contact details, support history	Legitimate interest in providing quality service
Marketing communications (email/newsletter)	Name, email	Consent
Service improvement, analytics	Usage data, technical data	Legitimate interest in improving services
Compliance with legal obligations	Any relevant personal data	Legal obligation
Funnel analysis and attribution (tracking effectiveness of advertising campaigns)	UTM campaign tags associated with user interactions on our website (without storing full referrer URLs or transmitting data externally)	Legitimate interest in analysing and improving marketing effectiveness

We may collect UTM parameters (such as campaign name, medium, or content) when you access our website through an advertising campaign. This information helps us understand how users progress through our service funnel and measure the effectiveness of our marketing efforts. We do not store the full external referrer URL. We do not combine UTM tags with other identifying information beyond what is necessary to assess user flows on our own website. We do not share UTM data with third parties in a way that would identify you personally. The lawful basis for this processing is our legitimate interest in analysing and improving the performance of our services and marketing campaigns, provided that such processing does not override your rights and freedoms.

Where we process special category data (e.g., passport copies, criminal record information), we do so only with your explicit consent or where necessary for the establishment of the service you requested. You may withdraw your consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.

Disclosure of your information

Information we share with third parties. We may share your information with selected third parties including:

Business partners, government bodies, suppliers and sub-contractors for the performance of any contract we enter into with them or you and for the purposes of providing part of the Platform or services to you. Such third parties supply the hardware infrastructure, consulting services, storage and associated services necessary for us to provide the Platform. All information submitted to third parties will be encrypted using secure SSL technology. By using our websites and/or the Platform you consent to our third-party service partners having access to your Personal Data.

Analytics and search engine providers that assist us in the improvement and optimization of our Platform.

We follow strict guidelines in the storage and disclosure of information that you have given us, to prevent unauthorized access. We comply with the laws of the countries from which we operate.

We may disclose your Personal Data to third parties:
If Migrun or substantially all of its assets are acquired by a third party, in which case Personal Data held by it about its customers will be unavoidably one of the transferred assets.
If we are under a duty to disclose or share your Personal Data in order to comply with any legal obligation, or in order to enforce or apply our Terms of Service and/or any other agreements; or to protect the rights, property, or safety of Migrun, our customers, or others. This includes exchanging information with other companies and organizations, government and other bodies for the purposes of fraud protection and legal compliance. In complying with court orders and similar legal processes, we strive for transparency. When permitted, we will make a reasonable effort to notify users of any disclosure of their information, unless we are prohibited by law or court order from doing so, or in rare, exigent circumstances.

Your Privacy Rights

Regardless of where you live, we believe you should have meaningful control over your personal data. We recognise and respect the rights you may have under applicable data protection laws in your country of residence or citizenship. The rights listed below are available to all our customers, subject to the limitations provided by applicable law.

If the laws of your country grant you additional or different rights beyond those listed here, you are free to exercise those rights, and we will comply with them to the extent required by applicable law.

You may exercise your rights at any time by contacting us at privacy@migrun.tech. We will respond to your request without undue delay and in any event within one (1) month of receipt. This period may be extended by up to two (2) additional months if necessary, taking into account the complexity and number of requests. If an extension is needed, we will inform you within the initial one-month period.

Your rights may include:
1. Access – The right to request a copy of the personal data we hold about you and information about how we process it.
2. Rectification – The right to request correction of inaccurate or incomplete personal data.
3. Erasure ("Right to be Forgotten") – The right to request deletion of your personal data, subject to legal or contractual retention requirements.
4. Restriction of Processing – The right to request that we temporarily or permanently stop processing all or some of your personal data.
5. Data Portability – The right to request a copy of your personal data in a structured, commonly used, machine-readable format and to have it transferred to another service provider where technically feasible.
6. Objection to Processing – The right to object to processing of your personal data for direct marketing purposes or, where permitted by law, to processing based on our legitimate interests.
7. No Automated Decision-Making and Profiling – The right not to be subject to a decision based solely on automated processing, including profiling, if it produces legal or similarly significant effects on you, unless permitted by applicable law.
8. Withdrawal of Consent – Where we rely on your consent for processing, the right to withdraw that consent at any time, without affecting the lawfulness of processing carried out before the withdrawal.
9. Right to Lodge a Complaint – The right to complain to a data protection authority or regulator.

Consent. If you wish to subscribe to our marketing communications, we will use your name and email address to send communications to you. We will inform you (before collecting your data) if we intend to use your data for such purposes or if we intend to disclose your information to any third party for such purposes. You may elect to stop receiving our marketing emails by following the unsubscribe instructions included in emails or simply notifying us on privacy@migrun.tech.

Questions, Concerns, and Complaints

If you have any questions or concerns about how we handle your personal data, or if you wish to exercise any of your privacy rights, you can contact us at privacy@migrun.tech or by registered mail at:
Migrantora Ltd – Lordou Vyronos 36, Nicosia Tower Center, 7th floor, 703, 1096, Nicosia, Cyprus.

We will investigate and respond to all complaints in accordance with applicable laws within applicable terms.

Please note that you may use any remedies available to you under applicable laws. If you believe that our processing of your personal data violates applicable privacy or data protection laws, you also have the right to seek a remedy or lodge a complaint with the competent data protection authority or other relevant regulator as applicable or otherwise.

Applicable Data Protection Law

For the purpose of data protection laws the data controller is Migrantora Ltd, a private limited company registered in Cyprus with its business registration number HE 481416, whose registered office is Lordou Vyronos 36, Nicosia Tower Center, 7th floor, 703, 1096, Nicosia, Cyprus.

Where we store your Personal Data

Cross-Border Data Transfers

Where we transfer personal data from the European Economic Area (EEA), the United Kingdom (UK), or Switzerland to a country outside those jurisdictions (including to our operations in Cyprus), such transfers are carried out in compliance with Chapter V of the General Data Protection Regulation (GDPR) and equivalent local laws.

If the European Commission (or the relevant UK or Swiss authority) has issued an adequacy decision for the destination country, we rely on that decision as the legal basis for the transfer. Where no adequacy decision exists, we use European Commission-approved Standard Contractual Clauses (SCCs) or, where applicable, Binding Corporate Rules (BCRs), to ensure that your personal data remains subject to a level of protection essentially equivalent to that provided under the GDPR.

Following best practices, we also conduct Transfer Impact Assessments (TIAs) for such transfers. These assessments consider the laws and practices of the destination country, the nature of the data, and the technical and organisational measures in place to protect it.

For transfers data, we implement additional safeguards, including encryption in transit and at rest, strict access controls, and confidentiality agreements with staff and service providers. We review these measures regularly to ensure that they continue to provide effective protection.

Migrun primarily stores Personal Information sent or collected via or by Migrun in the European Union, in the cloud, our servers, the servers of our group of companies, or the servers of our Service Providers. To facilitate our global operations, we may transfer and access such information from around the world. To carry out the email delivery function of the Platform, we may need to transfer such information around the world. Personal Information may be accessible to law enforcement or other authorities pursuant to a lawful request worldwide. By providing information to Migrun and continuing using the Platform, you explicitly consent to the transfer and storage of Personal Information in these locations.

Our Platform is accessible via the Internet and may potentially be accessed by any user around the world. Other users may access the Platform from outside the EEA. This means that where you chose to upload your data to the Platform, it could be accessed from anywhere around the world and therefore a transfer of your data outside of the EEA may be deemed to have occurred. You consent to such transfer of your data for and by way of this purpose.

Where we have given you (or where you have chosen) a password which enables you to access certain parts of the Platform, you are responsible for keeping this password confidential. We ask you not to share any password with anyone. Unfortunately, the transmission of information via the Internet is not completely secure. Although we will do our best to protect your Personal Data, we cannot guarantee the security of your data transmitted to our Platform; any transmission is at your own risk. Once we have received

your information, we will use strict procedures and security features to try to prevent unauthorised access. The Platform may contain links to and from third party websites of our partners, networks, advertisers, and affiliate. If you follow a link to any of these websites, please note that these websites have their own privacy policies, and we do not accept any responsibility or liability for the privacy practices or content of these websites.

Google API Services Disclosure

Migrun's use and transfer to any other app of information received from Google APIs will adhere to Google API Services User Data Policy, including the Limited Use requirements

Changes to This Privacy Policy

We reserve the right to change this Privacy Policy at any time and any amended Privacy Policy will be posted on our website and/or notified to you by email, where appropriate. Please check back frequently to see any updates or changes to our Privacy Policy. This Privacy Policy was last updated on 15 December 2025 and replaces any other Privacy Policy previously applicable from this date.

Contact us

Questions, comments and requests regarding this Privacy Policy are welcomed and should be forwarded by email to privacy@migrun.tech.