Privacy Notice

December 2025

Intermark Relocation ("Intermark", "we", "us", "our") respects your privacy and is committed to protecting your personal data.

This Privacy Notice explains how **Intermark** collects, uses, discloses and protects personal data when providing relocation, immigration, housing and mobility services.

It applies to all individuals whose data we process, regardless of location.

1. Data Controller Information

Intermark is a group of companies operating internationally.

The Intermark entity acting as the Data Controller will depend on the service you receive and your contractual relationship.

The following entities may act as Data Controller:

Intermark Corporate Services Limited (INTERMARK RELOCATION)
Registered address: Ground Floor, 123 Pall Mall, London, SW1Y 5EA
Company number: 9245817

Intermark Relocation Kazakhstan LLP
Registered address: 151A Zhamakayev Street, Medeu District, Almaty, 050010, Republic of Kazakhstan
Business Identification Number (BIN): 170240035637

Intermark Relocation Central Asia LLP
Registered address: Republic of Kazakhstan, Almaty city, Bostandyksky district, 280 Baizakova Street, non-residential premises No. 3, postal code 050040.
Business Identification Number (BIN): 230840005899

INTERMARK EUROPE DOO BEOGRAD
Registered address: Beograd, Omladinskih brigada 90V 6. sprat (6th floor) 11070
Company number: 21925624

Intermark Group companies apply the **same privacy, security and compliance standards,** and your data will be processed according to this Notice and applicable data protection laws, including the UK GDPR, EU GDPR (where applicable), and relevant local laws.

If you have questions or requests regarding our privacy practices, please contact:

The INTERMARK RELOCATION's Data Protection Officer is **Andrey Lukash**, A.Lukash@intermarkrelocation.com (Quality & Compliance).

1.1. Who This Privacy Notice Applies To

This Privacy Notice applies to you if we process your personal data in the context of our services, including (but not limited to):

- individual clients using our relocation, immigration, housing or mobility services;
- employees, contractors or assignees of corporate clients whose relocation or immigration is coordinated by Intermark;
- landlords, property owners and their representatives with whom we interact to arrange housing;
- vendors and service partners (for example movers, translators and other local providers);
- job applicants who apply for a position with Intermark;
- website visitors and any person who contacts us by email, phone or via online forms.

You may be located in the United Kingdom, the European Economic Area (EEA) or in another country. Regardless of your location, where this Notice applies, your personal data is processed under the responsibility of Intermark in accordance with this Privacy Notice and applicable data protection laws.

2. Categories of Personal Data We Process

We only collect personal data that is necessary for providing our relocation, immigration, housing, mobility, tenancy, and related support services. The categories of data we collect depend on who you are (for example, an individual client, a corporate assignee, a landlord, a vendor, or a job applicant) and on the specific services we are providing.

This section describes the types of information we collect and process.

2.1 Identification and Contact Information

We collect basic personal details that allow us to identify you and communicate with you, including:

- Full name, previous names
- Residential address or proof of address
- Email address(es)
- Mobile or other telephone numbers
- Date and place of birth
- Nationality and citizenship
- Signature (for immigration forms, tenancy documents, POAs, customs documents)

This information is essential for nearly all relocation and immigration procedures, tenancy negotiations and coordination of services.

2.2 Identity, Travel and Immigration Documentation

To provide immigration, visa, registration, customs or other regulatory services, we may collect information from your official documents, including:

- Passport details (number, issue/expiry date, issuing authority)
- Visa information (type, issuance, expiry, restrictions)
- Residence permits, migration cards, arrival/departure records
- Work permits or eligibility confirmations
- Power of attorney forms
- Scans or photos of identity documents (as required for lodging applications)

This data is often required under applicable immigration and customs laws.

2.3 Employment and Assignment Information

When services are provided in connection with a corporate relocation or assignment, we may process employment-related information provided by you or your employer, including:

- Job title and role
- Employer name and contact information
- Department, manager details and HR contacts
- Assignment letters and mobility authorisations
- Package details that affect relocation (e.g., housing allowances)
- Start/end dates of employment or assignment
- Internal approvals required to deliver services
- Details of accompanying family members

We use this information to verify eligibility, secure permits, and coordinate relocation benefits.

2.4 Housing and Tenancy Information

As part of housing search, tenancy negotiation, move-in/move-out services or property management support, we may collect:

- Property search preferences (location, budget, size, requirements)
- Employment confirmation letters related to tenancy
- Landlord or agent contact information
- Draft and signed tenancy agreements
- Details of utilities, access codes, handover documentation
- Records of inspections, maintenance, repairs or move-out findings

We also process personal data of **landlords and property owners**, including:

- Names and contact details
- ID or proof of ownership where required for contract procedures
- Banking details (when needed for rent transfer setup)

2.5 Family and Dependent Information

If your relocation or immigration case involves dependents, we may process:

- Names, dates of birth
- Birth certificates
- Relationship to you
- School preferences and education-related data
- Visa, passport and immigration data of dependents

We collect this information only when necessary to support family relocation or immigration.

2.6 Financial and Billing Information

We may process certain financial information for invoicing, reimbursement, expense coordination or payments, such as:

- Billing address and tax identifiers
- Payment confirmations
- Transaction records
- Bank details (for contractors and some vendors)
- Information required for customs duties, insurance, or financial guarantees

We **do not** store or process card details unless required for a specific transaction through a secure payment provider.

2.7 Communication Data

We maintain records necessary to manage your case and ensure continuity of services, including:

- Emails and correspondence between you and Intermark
- Messages exchanged through online forms or secure upload channels
- Notes from phone calls (where relevant to service delivery)
- Feedback provided during or after services
- Documents or attachments you voluntarily send to us

This allows us to manage your service file, document decisions and maintain quality and compliance.

2.8 Technical, Security and Website Data

When you visit our website or interact with our digital systems, we may collect:

- IP address and device identifiers
- Browser type, settings, and version
- Operating system and platform
- Log data (date, time, access records)
- Cookie and tracking information (see the Cookies section)
- Information collected through security tools designed to protect our environment

We collect this information to maintain security, detect anomalies, improve site functionality and ensure compliance with our technical security policies, including the Password Policy and Security Management Plan.

2.9 Special Category (Sensitive) Personal Data

We only collect special category data when strictly necessary and lawful for the services requested. These types of data may include:

- **Health information** (medical certificates required for visas or dependents)
- **Biometric data** (passport photos, scans, identification photos for immigration forms)
- **Marital status** (marriage/divorce certificates for immigration eligibility)
- **Dependent information** (including children's documents for school placement or visas)
- **Criminal-background-related documentation** if required by immigration authorities (e.g., police clearance certificates)

We process such data **only with explicit consent** or **where legally required** by immigration, customs or labor regulations.

2.10 Information We Receive from Third Parties

We may receive personal data from third parties directly involved in your relocation or housing process (such as your employer, landlords, authorities or service providers), as described in Section 3.

2.11 Children's Data

We do not intentionally collect data about individuals under 18 except:

- when they are dependents included in relocation or immigration cases, and
- only with parental or legal guardian authorization.

Personal data relating to children is retained only for as long as necessary to provide the relevant services and to comply with legal or audit requirements. For more information, see the Data Retention section of this Notice.

3. How We Collect Personal Data

We collect personal data in several ways, depending on the services you request and the context of our interaction with you. We only collect information that is relevant and necessary for providing relocation, immigration, housing, mobility, tenancy and related support services.

3.1 Data You Provide to Us Directly

Most of the personal data we process is provided directly by you. This may happen when you:

- complete questionnaires or service forms;
- provide documents for immigration, tenancy or customs purposes;
- correspond with us by email or phone;
- submit information through our website forms or secure upload channels;
- attend orientation, tenancy, immigration or other service-related meetings;
- give us feedback or request assistance;
- sign tenancy agreements, immigration forms or service documents.

We rely on the accuracy of the information you provide and may request updates when necessary for service delivery or regulatory compliance.

3.2 Data Provided by Your Employer (Corporate Relocation Cases)

If your employer engages Intermark to provide relocation or immigration services, we may receive your personal data directly from your employer, for example when your HR or mobility team submits a service request or authorises us to begin work on your case.

Your employer shares this information to enable us to provide the agreed services on your behalf. We rely on your employer to ensure that it has a lawful basis to disclose this data under applicable data protection laws.

3.3 Data Obtained from Third Parties as Part of Service Delivery

Depending on the services requested, we may receive personal data from third parties who are directly involved in your relocation or housing process, such as:

- landlords, property agents or building management;
- government and regulatory authorities (e.g., immigration, tax or customs bodies);

- service vendors and partners (e.g., movers, schools, translators, temporary accommodation providers);
- previously engaged landlords or agents where needed to complete tenancy procedures.

We receive only the information necessary to provide the requested services.

3.4 Data Collected Automatically When Using Our Website or Digital Tools

When you use our website or digital tools, technical and security data described in Section 2.8 may be collected automatically through logs, cookies and similar technologies. We use this data to keep our systems secure, ensure proper website functionality and improve performance, as described in the Cookies and Tracking section.

3.5 Data Obtained from Public or Official Sources

Where lawful and necessary, we may obtain information from:

- publicly accessible registers,
- official government databases,
- publicly available property or market listings,
- publicly available contact details relevant to service coordination.

We do not collect data from social media unless you provide it directly.

3.6 Data Collected Through Security and Compliance Measures

To protect our systems and meet compliance requirements, we may process system-generated security data. This processing is limited to security, monitoring and fraud-prevention purposes and follows our internal information security policies.

3.7 Data Provided by Someone Acting on Your Behalf

In certain cases, your personal data may be provided to us by someone authorised to act on your behalf, such as:

- your employer,
- a spouse, parent or legal guardian,
- a legal representative or a person with power of attorney,
- a colleague assisting with coordination.

We process such data only to provide the requested services.

All data collection is transparent and connected to providing our services.

4. Purposes of Processing and Legal Bases

Intermark processes personal data in accordance with the UK GDPR. Where the personal data we process relates to individuals protected under the EU GDPR, Intermark applies EU GDPR requirements to this processing even if the person or organization providing the data is not itself subject to the EU GDPR.

The tables below summarize the purposes for which we process personal data and the lawful bases we rely on under the UK GDPR and, where applicable, the EU GDPR.

4.1 Relocation, Immigration and Regulatory Services

Purpose	Legal Basis
Delivering relocation, immigration and registration services	UK GDPR: Art. 6(1)(b) EU GDPR: Art. 6(1)(b)
Preparing and submitting immigration, visa or customs documents	UK GDPR: Art. 6(1)(c) EU GDPR: Art. 6(1)(c)
Identity and document verification	UK GDPR: Art. 6(1)(b)/(c) EU GDPR: Art. 6(1)(b)/(c)
Coordination with authorities and service partners	UK GDPR: Art. 6(1)(b)/(f) EU GDPR: Art. 6(1)(b)/(f)
Case management and communication records	UK GDPR: Art. 6(1)(b)/(f) EU GDPR: Art. 6(1)(b)/(f)
Processing dependent information	UK GDPR: Art. 6(1)(b); Art. 9(2)(a) (if applicable) • EU GDPR: same

4.2 Housing and Tenancy Services

Purpose	Legal Basis
Housing search, viewings, tenancy coordination	UK GDPR: Art. 6(1)(b) EU GDPR: Art. 6(1)(b)
Preparing tenancy documents	UK GDPR: Art. 6(1)(b) EU GDPR: Art. 6(1)(b)
Move-in/out coordination and landlord communication	UK GDPR: Art. 6(1)(b)/(f) EU GDPR: Art. 6(1)(b)/(f)
Meeting statutory housing requirements	UK GDPR: Art. 6(1)(c) EU GDPR: Art. 6(1)(c)

4.3 Logistics, Customs and Move Management

Purpose	Legal Basis
Coordinating packing, transport, storage and delivery	UK GDPR: Art. 6(1)(b) EU GDPR: Art. 6(1)(b)
Preparing customs forms, supporting clearance	UK GDPR: Art. 6(1)(c) EU GDPR: Art. 6(1)(c)
Communication with logistics vendors	UK GDPR: Art. 6(1)(b)/(f) EU GDPR: Art. 6(1)(b)/(f)

4.4 Corporate Client and Assignment Management

Purpose	Legal Basis
Updates and reporting to corporate clients	UK GDPR: Art. 6(1)(f) EU GDPR: Art. 6(1)(f)
Confirming entitlements and assignment details	UK GDPR: Art. 6(1)(b)/(f) EU GDPR: Art. 6(1)(b)/(f)
Compliance with employer mobility policies	UK GDPR: Art. 6(1)(f) EU GDPR: Art. 6(1)(f)

4.5 Communications and Service Support

Purpose	Legal Basis
Responding to enquiries and managing correspondence	UK GDPR: Art. 6(1)(b)/(f) EU GDPR: Art. 6(1)(b)/(f)
Maintaining service records for continuity	UK GDPR: Art. 6(1)(b)/(f) EU GDPR: Art. 6(1)(b)/(f)
Service-quality feedback	UK GDPR: Art. 6(1)(f) EU GDPR: Art. 6(1)(f)

4.6 Website, Cookies and IT Security

Purpose	Legal Basis
Operating and improving website functionality	UK GDPR: Art. 6(1)(f) EU GDPR: Art. 6(1)(f)
Strictly necessary cookies	UK GDPR: Art. 6(1)(f) EU GDPR: Art. 6(1)(f)
Analytics / marketing cookies	UK GDPR: Art. 6(1)(a) EU GDPR: Art. 6(1)(a)
IT security monitoring, logs, fraud prevention	UK GDPR: Art. 6(1)(c)/(f) EU GDPR: Art. 6(1)(c)/(f)

4.7 Recruitment and Job Applicants

Purpose	Legal Basis
Reviewing applications and assessing candidates	UK GDPR: Art. 6(1)(f) EU GDPR: Art. 6(1)(f)
Communication with candidates	UK GDPR: Art. 6(1)(f) EU GDPR: Art. 6(1)(f)
Talent pool retention with consent	UK GDPR: Art. 6(1)(a) EU GDPR: Art. 6(1)(a)

4.8 Special Category Data

Purpose	Legal Basis
Processing health, biometric or dependent information for immigration/relocation	UK GDPR: Art. 9(2)(a) + Art. 6(1)(b)/(c) EU GDPR: same
Processing special category data required by law or substantial public interest	UK GDPR: Art. 9(2)(g) + Art. 6(1)(c) EU GDPR: same

4.9 Legal and Compliance Obligations

Purpose	Legal Basis
Tax, accounting, audit and statutory compliance	UK GDPR: Art. 6(1)(c) EU GDPR: Art. 6(1)(c)
Responding to lawful authorities	UK GDPR: Art. 6(1)(c) EU GDPR: Art. 6(1)(c)
Establishing or defending legal claims	UK GDPR: Art. 6(1)(f) EU GDPR: Art. 6(1)(f)

5. Data Recipients

Intermark shares personal data only where necessary for delivering services, meeting legal requirements, or supporting our operational processes. Each recipient receives only the minimum data needed for their role, and where they act as processors, they do so under written agreements compliant with the UK GDPR and the EU GDPR.

5.1 Service Providers Involved in Service Delivery

Depending on the services requested, data may be shared with:

- public authorities responsible for immigration, visas, registration, taxation or customs;
- property owners, agents and building management involved in tenancy arrangements;
- moving companies, logistics partners and storage facilities;
- temporary accommodation providers, schools and educational institutions (where requested);
- certified translators, notaries and document-processing providers.

5.2 Corporate Clients

Where services are initiated and paid for by your employer, we may share relevant information with authorised representatives of that employer for the purposes of service coordination and reporting in line with the corporate relocation programme.

5.3 IT and Cloud Service

We use third-party IT and cloud service providers to host our systems, support secure communication, enable case management, and facilitate document exchange. These providers act as data processors on behalf of the Intermark Group entity responsible for your data. They can process personal data only on documented instructions from that entity and must apply appropriate contractual and technical safeguards to protect the data.

5.4. Public Authorities and Regulators

Intermark may disclose personal data to competent authorities where legally required, including immigration authorities, courts, regulators or tax bodies acting under statutory powers.

5.5 Third Parties Authorised by You

We may share personal data with third parties where:

- you have explicitly instructed us to do so,
- you have authorised a representative to act on your behalf,
- a legal representative acts under a power of attorney or similar authority.

6. International Transfers of Personal Data

Because Intermark provides relocation, immigration, housing and mobility services in multiple countries, we may need to transfer your personal data to organizations located outside the United Kingdom or the European Union. This may also include sharing certain personal data within Intermark Group entities where required to deliver the relevant services. All such transfers are limited to what is necessary, made only for service-related purposes, and are carried out subject to appropriate safeguards. Intermark does not transfer personal data for marketing or any unrelated purposes.

6.1 When International Transfers Take Place

International transfers may occur, for example, when:

- submitting documents to consulates or immigration authorities abroad;
- coordinating with landlords, schools, relocation partners or service providers in another country;
- arranging accommodation, transportation or local support services;
- handling documentation required by foreign authorities or institutions.

We share only the minimum data required for each specific task.

6.2 Legal Basis for International Transfers

Where required by data protection laws, Intermark uses legally recognized mechanisms for international transfers. The applicable mechanism depends on the destination country and the nature of the transfer.

6.3 Ensuring Adequate Protection

For transfers to countries that do not benefit from an adequacy decision, Intermark applies safeguards permitted under the UK GDPR and, where applicable, the EU GDPR. These safeguards aim to ensure that personal data continues to receive an appropriate level of protection.

Further information about how Intermark protects personal data, including our technical and organizational security measures, is provided in Section 7 (Data Security).

6.4 Your Right to Know More

You may request further information about international transfers and applicable safeguards at any time using the contact details in Section 1.

7. Data Security

Intermark takes the protection of your personal data seriously. We apply a combination of technical and organizational measures to keep your information secure and to ensure it is handled appropriately throughout the delivery of our services.

These measures reflect our internal policies, including the Data Protection Policy, Information Security Management Plan, Data Classification Policy, User Access Control Policy, Password Policy, Backup & Recovery Policy, Incident Response Plan, Cyber Security Management Policy and related procedures.

7.1 How We Protect Your Information

We maintain controls designed to prevent unauthorized access, accidental loss or misuse of personal data. These include:

- access to systems and data based on role and business need;
- secure handling, storage and disposal of documents and electronic records;
- procedures ensuring that only authorized staff and partners may process personal data;
- measures supporting the availability and integrity of systems that hold personal data.

7.2 Staff Responsibilities and Training

All employees who handle personal data are subject to confidentiality obligations and are required to follow our internal policies. Staff receive training on data protection and information security relevant to their responsibilities.

7.3 Responding to Security Incidents

Intermark maintains an incident response process that allows us to identify, assess and respond to suspected or actual security incidents. Where required by law, we will notify affected individuals and the relevant supervisory authority of a personal data breach.

7.4 Physical Security

Our offices and storage areas are restricted to authorized personnel, and documents or equipment containing personal data are kept securely to prevent unauthorized access.

7.5 Continuous Review and Improvement

We regularly review our security practices, assess risks and update our controls to reflect legal requirements, operational changes and industry standards.

7.6 Personal Data Incidents and Breach Notifications

Despite the security measures we apply, incidents involving personal data may still occur. Intermark maintains internal procedures for detecting, reviewing and responding to such incidents.

If we become aware of a personal data incident, we will:

- assess what happened and which data may be affected;
- evaluate whether the incident creates a risk or high risk to individuals;
- take steps to contain the incident and prevent further unauthorised access or disclosure.

Where required by applicable law, we will:

- notify the competent supervisory authority **within the timelines set by law**; and
- notify affected individuals **without undue delay** where the incident is likely to result in a high risk to their rights and freedoms.

When we inform you about an incident, we will explain in clear language:

- what happened in general terms;
- what types of personal data may be affected;
- what measures we have taken or plan to take; and
- what steps you can take to protect yourself, if relevant.

Following an incident, we also review the underlying cause and implement appropriate corrective and preventive measures (for example, strengthening

technical safeguards, updating procedures or providing additional staff training) to reduce the likelihood of similar events in the future.

8. Compliance Monitoring and Policy Updates

Intermark regularly reviews its data protection practices to ensure that our processing of personal data remains compliant with applicable laws.

Our Data Protection Officer, together with the Legal Department, monitors changes in legislation and regulatory guidance and updates our internal procedures where necessary.

We review this Privacy Notice and our internal data protection policies **at least once per year**, or sooner if legal or operational changes require it.

When updates are made, they are:

- approved by senior management,
- published on our corporate portal, and
- communicated to employees through internal notifications or training.

The most recent review date of this Privacy Notice is indicated at the end of the document.

9. Data Retention

Intermark keeps personal data only for as long as it is reasonably necessary for the purposes for which it was collected or for which it is further processed. We do not retain personal data longer than necessary and do not keep records without a valid legal, regulatory or operational reason.

Retention periods may vary depending on which Intermark Group entity acts as the data controller and the legal requirements of the jurisdiction governing the processing.

9.1 How We Decide How Long to Keep Data

Retention periods are determined with reference to:

- the duration of the relocation, immigration, housing or mobility services and a limited period afterwards (for follow-up, support and quality purposes);
- statutory requirements (for example, accounting, tax, corporate or immigration record-keeping obligations);
- the time needed to establish, exercise or defend legal claims;
- internal audit, compliance and risk-management needs, where justified.

These rules are set out in Intermark's internal Data Retention Policy and associated retention schedules.

9.2 Categories of Data

In practice, this means that:

- service files and supporting documents are kept for a limited period after service completion, in line with legal and operational requirements;
- financial and invoicing data are kept for the period required by applicable accounting and tax laws;
- immigration-related records are kept only for as long as necessary to demonstrate compliance with legal obligations or to respond to audits or inspections;
- communications and correspondence are kept only while they are needed to document service delivery or resolve issues.

Specific retention periods may vary depending on the service, the country involved and the type of data.

9.3 Deletion and Anonymisation

When personal data is no longer required, Intermark applies secure deletion or anonymisation procedures in line with our Data Retention Policy and information security requirements.

10. Your Data Protection Rights

Depending on applicable data protection law, you have several rights in relation to your personal data. You may exercise these rights at any time by contacting Intermark using the details in Section 1. We may need to verify your identity before responding to your request.

10.1 Right of Access

You may request a copy of the personal data we hold about you, along with information about how we process it.

10.2 Right to Rectification

You may ask us to correct or complete personal data that is inaccurate or incomplete.

10.3 Right to Erasure

You may request the deletion of your personal data where there is no valid reason for us to continue processing it. This right may not apply where we must retain data for legal, regulatory or contractual reasons.

10.4 Right to Restriction

You may ask us to limit the processing of your personal data in certain circumstances — for example, while we verify accuracy or assess an objection.

10.5 Right to Object

You may object to processing based on legitimate interests, unless we can demonstrate compelling reasons to continue. You may always object to direct marketing.

10.6 Right to Data Portability

Where processing is based on consent or contract and carried out by automated means, you may request your data in a structured, commonly used and machine-readable format, and you may ask us to transfer it to another controller where technically feasible.

10.7 Right to Withdraw Consent

If we rely on consent to process your data, you may withdraw it at any time. This does not affect the lawfulness of processing before withdrawal.

10.8 Right Not to Be Subject to Automated Decisions

Intermark does not make decisions that produce legal or similarly significant effects solely through automated processing. If this changes, we will notify you and explain your related rights.

10.9 How to Exercise Your Rights

We aim to respond to all valid requests within one month. Complex or numerous requests may take longer, in which case we will inform you. We may decline a request where permitted by law — for example, if complying would affect the rights of others or if data must be retained for legal reasons.

You also have the right to lodge a complaint with a supervisory authority (see Section 10).

11. How to Submit a Privacy Complaint

If you have concerns about how Intermark processes your personal data, you may contact us using the details in Section 1.

When we receive a complaint, we:

1. **Acknowledge receipt within five (5) working days;**
2. **Review the issue,** which may include requesting additional information;
3. **Provide a response within one (1) month,** in line with applicable data protection laws. (For complex matters, this period may be extended by up to two additional months; we will inform you if this is necessary.)

If we identify an error or non-compliance, we will take appropriate corrective steps. You also have the right to contact the relevant supervisory authority (see below).

12. Supervisory Authority and Complaints

If you have concerns about how Intermark processes your personal data, we encourage you to contact us first using the details in Section 1 so we can address your query.

You also have the right to lodge a complaint with a data protection authority. Your applicable supervisory authority depends on which Intermark Group entity acts as your data controller and on the data protection laws governing the relevant processing.

12.1 United Kingdom

If your data is processed under the UK GDPR or if your data controller is a UK-based Intermark entity, you have the right to lodge a complaint with the UK supervisory authority:

Information Commissioner's Office (ICO)
Website: www.ico.org.uk
Telephone: +44 303 123 1113

12.2 European Union

If the EU GDPR applies to your personal data, you may submit a complaint to the data protection authority in the EU Member State of your habitual residence, place of work or where you believe a violation occurred.

A list of EU authorities is available at:
https://edpb.europa.eu/about-edpb/board/members_en

You may exercise this right without prejudice to any other administrative or judicial remedy.

12.3 Kazakhstan Supervisory Authority

If your data controller is Intermark Relocation Kazakhstan LLP or Intermark Relocation Central Asia LLP, or if your personal data is processed under the laws of the Republic of Kazakhstan, you may contact the national supervisory authority:

Committee for Information Security
Ministry of Digital Development, Innovations and Aerospace Industry
of the Republic of Kazakhstan
Address: 55/14 Mangilik El Avenue, Astana, Republic of Kazakhstan, 010000
Phone: 8 (7172) 61-33-25, 61-33-23
e-mail: moap@mdai.gov.kz
Website: https://www.gov.kz/memleket/entities/maidd?lang=en

12.4 Serbia

If your data controller is Intermark Europe d.o.o. Serbia, or if your personal data is processed under the Serbian Law on Personal Data Protection, you have the right to lodge a complaint with the Serbian supervisory authority:

Commissioner for Information of Public Importance and Personal Data Protection (Poverenik)
Address: Bulevar kralja Aleksandra 15, 11000 Belgrade, Serbia
Website: https://www.poverenik.rs
Email: office@poverenik.rs
Phone: +381 11 3408 900

13. Cookies and Tracking Technologies

Our website uses cookies and similar technologies to ensure it functions properly and to help us understand how visitors use it. Cookies are small files placed on your device when you browse a website. They support essential functions and can also help us improve site performance.

13.1 Types of Cookies We Use

We may use the following categories:

- Strictly necessary cookies – required for core website functions.
- Analytical/performance cookies – help us understand how visitors interact with our site.
- Functional cookies – remember your preferences (such as language or region).

We do **not** use cookies for targeted advertising.

13.2 How We Use Consent

Where required by law, we ask for your consent before placing non-essential cookies.
You can change or withdraw your cookie preferences at any time through your browser or our cookie banner.

13.3 Managing Cookies

Most browsers allow you to block or delete cookies. If you do so, some website features may not function as intended.

14. Changes to This Privacy Notice

We may update this Privacy Notice from time to time to reflect changes in our services, legal requirements or internal practices. When updates are made, the "Last Updated" date at the end of this Notice will be amended. If any changes significantly affect how we process personal data, we may provide additional notice where appropriate.

15. Effective Date and Review Cycle

This Privacy Notice is reviewed at least once per year, or earlier if changes in our services or legal requirements make an update necessary.