

Privacy Policy

Last Updated: January 2026

Effective Date: Immediately upon publication

1. Introduction

This Privacy Policy (“**Policy**”) describes how **NetLir LTD** (“**NetLir**”, “**we**”, “**our**”, or “**us**”) collects, uses, stores, and protects personal data when individuals and organizations (“**you**”, “**your**”, or “**the Client**”) access or use our website <https://netlir.pro>, the NetLir Customer Portal, or any of our related products and services (collectively referred to as the “**Services**”).

NetLir LTD is a private limited company registered in **England and Wales** under company number **16465349**, with its registered office at:

71–75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom.

We recognize the importance of protecting personal information and are committed to handling it responsibly and transparently in accordance with:

- the **UK General Data Protection Regulation (UK GDPR)**;
- the **Data Protection Act 2018**; and
- any other applicable data protection or privacy legislation.

Depending on the nature of the activity, **NetLir acts as**:

- a **Data Controller** — when we determine the purpose and means of processing personal data (e.g., for client accounts, billing, and service management); and
- a **Data Processor** — when processing personal data on behalf of clients for specific purposes, such as managing RIPE NCC objects, maintaining database entries, or fulfilling compliance obligations as a sponsoring LIR.

This Policy explains:

- what personal data we collect and how we obtain it;
- the purposes and legal bases for processing it;
- how long we retain it and how we protect it;
- your rights under the applicable data protection laws; and
- how you can contact us regarding privacy-related questions or concerns.

By using our website, ordering our services, registering an account, or otherwise communicating with us, you confirm that you have read, understood, and agreed to this Policy.

If you do not agree with this Policy or any part of it, please refrain from using our website or Services.

NetLir reserves the right to amend this Policy from time to time. Updates will be published on our website, and the “Last Updated” date at the top will indicate the most recent revision.

2. Data We Collect

To provide our Services, fulfill contractual and legal obligations, and maintain compliance with RIPE NCC policies, **NetLir LTD** may collect, store, and process both **personal** and **organizational** data.

We do not collect more information than is necessary and always process it lawfully, fairly, and transparently.

2.1. Information You Provide Directly

We collect personal and company information that you voluntarily provide when communicating with us, registering an account, placing an order, or submitting documentation. This includes:

- **Identification and contact information:** full name, company name, job title, email address, postal address, and phone number;
- **Account and billing information:** VAT number, bank or payment reference, billing address, payment status, and transaction history;
- **RIPE NCC–related data:** organization ID, Autonomous System Number (ASN), network contact details, maintainer information, and role accounts (e.g., admin-c, tech-c, abuse-c);
- **Verification and compliance data:** company registration documents, identification of authorized persons, or proof of address as required under KYC/KYB procedures;
- **Communications and correspondence:** email exchanges, support tickets, abuse reports, service requests, and audit-related documentation submitted to our team.

2.2. Information Collected Automatically

When you access our website, portal, or online systems, we automatically collect limited technical information to ensure functionality, security, and performance. This may include:

- **Technical identifiers:** IP address, device type, operating system, browser version, and connection metadata;
- **Access and activity logs:** timestamps, login records, API usage, and resource access patterns;
- **Cookies and similar technologies:** session identifiers, authentication tokens, and analytics data used to secure the website and analyze aggregate trends;
- **Error logs and diagnostic data:** automatically recorded system events to identify performance issues or unauthorized access attempts.

We do not use automated decision-making or profiling that produces legal or significant effects on individuals.

2.3. Information Obtained from Third Parties

In some cases, we may receive or verify data through third parties where permitted by law, including:

- **RIPE NCC:** for validation of existing LIR or ASN resources, compliance checks, and database synchronization;

- **Payment processors and banks:** to confirm transaction authenticity and prevent fraudulent activity;
- **Public registries:** such as *Companies House* or other corporate databases, to validate company registration and ownership information;
- **Compliance and due diligence providers:** to support anti-fraud, anti-abuse, and sanctions screening obligations.

2.4. Sensitive Data

NetLir does not intentionally collect or process **special categories of personal data** (such as racial or ethnic origin, political opinions, religious beliefs, health information, or biometric data).

If such data is inadvertently submitted (e.g., in uploaded documents), it will be securely deleted unless processing is required by law or for compliance purposes.

2.5. Accuracy and Responsibility

You are responsible for ensuring that all data you provide to NetLir is **accurate, complete, and up to date**.

We rely on this accuracy to fulfill our contractual and regulatory obligations effectively.

3. Purpose and Legal Basis for Processing

We process personal and organizational data only when there is a **lawful basis** under the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

Each category of processing activity corresponds to one or more legal bases described below.

3.1. Overview of Processing Purposes

Purpose of Processing	Description	Legal Basis (UK GDPR Article 6)
Account setup and service delivery	Creating and managing client accounts, verifying identity, allocating IP resources, and providing LIR or ASN services.	Contractual necessity – processing is required to perform a contract with the Client.
Billing and financial transactions	Issuing invoices, processing payments, managing subscriptions, and keeping financial records.	Legal obligation (tax/accounting laws) and contractual necessity .
Communication and support	Responding to inquiries, providing technical support, and notifying Clients about service updates or outages.	Legitimate interest – ensuring efficient customer service and communication.
Compliance with RIPE NCC policies	Maintaining accurate WHOIS and RIPE database objects, performing audits, and verifying resource usage.	Legal obligation – required under RIPE NCC policy and data accuracy regulations.
Fraud prevention and abuse control	Detecting, investigating, and preventing network abuse, spam, or unauthorized activities.	Legitimate interest – maintaining security and protecting infrastructure.

Purpose of Processing	Description	Legal Basis (UK GDPR Article 6)
Administrative notices and updates	Sending important service-related messages, renewals, or policy changes.	Contractual necessity – essential to maintain service continuity.
Internal record keeping and audits	Storing historical data for RIPE NCC audits, legal compliance, and operational integrity.	Legal obligation and legitimate interest – ensuring compliance and accountability.
Website analytics and security monitoring	Monitoring site performance, analyzing usage trends, detecting anomalies, and improving service quality.	Legitimate interest – optimizing user experience and securing infrastructure.
Marketing communications (optional)	Sending newsletters or informational updates about NetLir’s services, only where permitted.	Consent – obtained explicitly and can be withdrawn at any time.

3.2. Contractual and Legal Obligations

Processing certain personal data (such as name, company information, payment data, or contact details) is necessary to enter into and perform a service contract.

Without this information, NetLir may be unable to provide or maintain its Services.

We are also required by law to retain certain records for accounting, taxation, and compliance purposes, as well as to fulfill RIPE NCC policy requirements regarding resource registration and verification.

3.3. Legitimate Interests

Where processing is based on **legitimate interest**, we ensure that:

- it is proportionate and necessary for our business operations;
- it does not override the rights and freedoms of data subjects;
- Clients always have the right to object to such processing as outlined in **Section 9 (Your Data Protection Rights)**.

3.4. Consent-Based Processing

Where consent is required (e.g., for marketing emails), we obtain it clearly and explicitly. Clients may withdraw consent at any time by contacting **support@netlir.pro** or using the unsubscribe link provided in communications.

4. How We Use and Share Data

4.1. Purpose of Use

NetLir processes and utilizes collected personal and organizational data solely for the purposes necessary to operate, maintain, and improve its Services in a lawful, secure, and transparent manner.

We use personal data to:

- **Provide and manage LIR sponsorship and IP resource allocations** under RIPE NCC policies;
- **Register and maintain RIPE NCC database objects** (including `inetnum`, `route`, `domain`, and `organisation` records);
- **Administer client accounts**, process payments, and maintain service-related communication;
- **Ensure technical and policy compliance** with RIPE NCC, network routing standards, and data accuracy requirements;
- **Respond to client inquiries**, support requests, and compliance verifications;
- **Detect, investigate, and prevent misuse, spam, network abuse, or fraudulent activity**;
- **Improve our website, portal, and service reliability** through analytics and technical monitoring;
- **Fulfil contractual and legal obligations**, including tax, accounting, and regulatory requirements.

We never use personal data for automated decision-making or profiling that produces legal or significant effects on individuals.

4.2. Sharing and Disclosure of Data

NetLir shares personal and organizational data only where necessary and always under secure and lawful conditions.

Such disclosures are limited to trusted third parties that perform essential functions required for service delivery.

We may share personal data with:

- **RIPE NCC** – for the registration, sponsorship, or verification of Internet number resources and for compliance with applicable RIPE policies.
This may include publication of limited information (such as organization name, maintainer handle, or contact email) in the **RIPE Database**, as required under RIPE's Terms and Conditions.
- **Payment processors and financial institutions** – to handle billing, invoicing, and fraud prevention.
Payment providers process only the minimum required information to authorize transactions securely.
- **Hosting, IT, and infrastructure providers** – who operate and maintain our systems, servers, backup environments, and email services.
All such partners are contractually bound by strict confidentiality and data protection obligations.
- **Auditors, consultants, or legal representatives** – where necessary for accounting, compliance, or dispute resolution purposes.

- **Regulatory or law enforcement authorities** – where disclosure is legally mandated, for example to comply with court orders, tax investigations, or data protection authorities.

4.3. Data Processing by Third Parties

Whenever personal data is shared with external providers or processors:

- access is restricted strictly to the data necessary for their specific function;
- processing is governed by a written **Data Processing Agreement (DPA)** ensuring compliance with the **UK GDPR**;
- all partners are required to implement robust **technical and organizational safeguards** to protect the integrity and confidentiality of data.

4.4. Cross-Border Data Transfers

If NetLir transfers personal data outside the **United Kingdom** or the **European Economic Area (EEA)**, we ensure that adequate protection is provided through:

- the use of **Standard Contractual Clauses (SCCs)** approved by the UK ICO or European Commission;
- transfer to jurisdictions recognized as providing **adequate data protection**; or
- other appropriate safeguards permitted by applicable law.

Clients may request a copy of the relevant safeguards by contacting support@netlir.pro.

4.5. Commitment to Data Confidentiality

NetLir strictly prohibits the sale, rental, or commercial exchange of personal or organizational data.

We do not disclose personal data to third parties for advertising or unrelated marketing purposes.

All data sharing activities are conducted on the basis of **necessity, proportionality, and legitimate purpose**, aligned with our commitment to transparency and accountability.

5. Data Transfers

5.1. Primary Processing Location

All personal data collected and processed by **NetLir LTD** is primarily stored, managed, and processed within the **United Kingdom** and the **European Economic Area (EEA)**. These regions provide a high level of data protection aligned with the requirements of the **UK GDPR** and **EU GDPR**, ensuring that personal information remains secure and lawfully managed.

5.2. Transfers Outside the UK and EEA

In certain cases, it may be necessary to transfer personal data to service providers, affiliates, or partners located **outside the United Kingdom or EEA**, for example:

- when using secure cloud or hosting services based in non-EEA countries;
- when engaging international technical or compliance support;
- when communicating with RIPE NCC partners or third parties operating globally.

Such transfers are limited to what is **strictly necessary** for the performance of contractual or operational obligations.

5.3. Safeguards for International Transfers

Whenever data is transferred to a third country, NetLir ensures that appropriate **legal and technical safeguards** are in place to maintain equivalent protection to that afforded under the UK GDPR.

These may include one or more of the following mechanisms:

- **Standard Contractual Clauses (SCCs):**
We enter into legally binding agreements incorporating the UK or EU-approved SCCs to ensure data recipients outside the UK/EEA provide adequate protection.
- **Adequacy Decisions:**
Transfers may occur to countries formally recognized by the **UK Government** or the **European Commission** as providing an adequate level of data protection (e.g., Canada, Japan, New Zealand).
- **Binding Corporate Rules (BCRs):**
Where transfers occur within a corporate group or affiliated entities, data is protected under internal rules approved by the relevant supervisory authority, ensuring consistent compliance across jurisdictions.
- **Alternative Safeguards:**
In rare cases where no formal adequacy decision or SCCs apply, we rely on limited exceptions under Article 49 of the UK GDPR — such as explicit client consent, necessity for contract performance, or legal obligations.

5.4. Technical and Organizational Measures

All international transfers are conducted using **secure communication channels** (e.g., encrypted connections, VPNs, or protected APIs).

We require all external processors to:

- comply with our data protection and confidentiality standards;
- limit access strictly to the data necessary for their function;
- implement robust **data security, retention, and deletion procedures**.

5.5. Client Rights and Transparency

Clients may request further details about:

- the specific countries where data is processed or stored;
- the legal basis for transfer; or
- copies of applicable safeguards (e.g., Standard Contractual Clauses).

Requests can be directed to support@netlir.pro.

NetLir will provide relevant information unless disclosure would compromise security or commercial confidentiality.

6. Data Retention

6.1. General Principle

NetLir LTD retains personal and organizational data **only for as long as necessary** to achieve the purposes for which it was collected, to comply with legal or regulatory obligations, and to maintain accurate business and compliance records.

Once the applicable retention period expires, data is securely deleted, anonymized, or archived in accordance with our internal Data Retention and Destruction Policy.

We never keep data longer than required and periodically review our storage systems to ensure compliance with the **storage limitation principle** under Article 5(1)(e) of the UK GDPR.

6.2. Standard Retention Periods

Unless otherwise required by law or RIPE NCC policy, we apply the following standard retention periods:

Category of Data	Retention Period	Purpose / Legal Basis
Account and billing records	7 years	Required for tax, accounting, and audit compliance under UK law (Finance Act 1998).
RIPE NCC documentation	5 years after service termination	Proof of resource allocation, sponsorship, and policy compliance for RIPE NCC audits.
Client contracts, LOAs, and service agreements	5 years after contract end	Legal defense, reference for renewals, and compliance verification.
Support and communication records (emails, tickets)	Up to 2 years	Service quality assurance and dispute resolution.
Technical and access logs (portal, API, infrastructure)	6 months	Security monitoring, incident analysis, and abuse prevention.
Abuse and compliance reports	Up to 3 years	Tracking of repeated violations, ensuring lawful use of IP resources.
Marketing or newsletter data	Until consent withdrawal or inactivity after 24 months	Based on explicit consent (Article 6(1)(a) UK GDPR).

6.3. Legal and Regulatory Retention

Certain records may be retained beyond the standard periods where:

- required by **law enforcement, tax authorities, or regulatory agencies**;
- necessary for the establishment, exercise, or defense of legal claims;
- requested by **RIPE NCC** for audit or policy compliance purposes.

In such cases, access to archived data is restricted strictly to authorized personnel.

6.4. Secure Deletion and Anonymization

Upon expiration of the retention period, NetLir ensures that personal data is:

- **permanently deleted** using certified data erasure procedures; or
- **irreversibly anonymized**, so that individuals can no longer be identified directly or indirectly.

Anonymized data may be used for statistical or analytical purposes without further notice to data subjects.

6.5. Client-Initiated Deletion

Clients may request deletion of personal data at any time by contacting support@netlir.pro, subject to legal or contractual limitations.

Where data must be retained for regulatory compliance, it will be securely isolated and restricted from operational processing.

7. Data Security

7.1. Commitment to Data Protection

NetLir LTD is committed to maintaining the confidentiality, integrity, and availability of all personal and organizational data processed through its systems.

We implement a combination of **technical, organizational, and procedural** measures designed to protect data against unauthorized access, alteration, disclosure, or destruction.

Our security practices are regularly reviewed and updated to meet evolving legal, regulatory, and technological standards.

7.2. Technical Security Measures

To protect data stored and transmitted through our systems, NetLir employs multiple layers of defense, including:

- **Encrypted data transmission (SSL/TLS):**
All communication between users and our servers is encrypted using industry-standard Transport Layer Security (TLS) to prevent interception and unauthorized access.
- **Secured data storage:**
All databases, file systems, and backups are protected by encryption at rest and hosted on secure infrastructure with restricted administrative access.
- **Access controls and authentication:**
Access to personal data is restricted to authorized employees and contractors under

the principle of **least privilege**.

Multi-factor authentication (2FA) is required for all administrative and customer portal accounts.

- **Network and application security:**

Firewalls, intrusion detection systems (IDS), and rate-limiting controls are used to monitor and block unauthorized activity.

Our systems undergo regular patching, code reviews, and vulnerability testing.

- **Backups and disaster recovery:**

Encrypted backups are maintained in geographically separate data centers to ensure data recovery in case of accidental loss or system failure.

7.3. Organizational and Procedural Safeguards

NetLir maintains internal policies and training programs to ensure that all personnel handling personal data are aware of their responsibilities and act in accordance with the **UK GDPR** and company procedures.

These include:

- Mandatory confidentiality agreements for all staff and contractors;
- Access logging and continuous monitoring of system activity;
- Periodic **security audits**, penetration tests, and compliance assessments;
- Clear incident response and escalation procedures.

7.4. Incident Response and Breach Management

In the event of a suspected or confirmed security incident involving personal data, NetLir will:

1. Immediately isolate affected systems and assess the scope of impact;
2. Notify internal data protection officers and, where applicable, the **Information Commissioner's Office (ICO)** within **72 hours** of becoming aware of the breach;
3. Inform affected clients without undue delay, providing details of the nature of the breach, potential risks, and recommended mitigation steps.

7.5. Client Responsibilities

While NetLir takes extensive measures to secure its infrastructure, **no online system can be guaranteed to be completely secure**.

Clients are responsible for:

- maintaining the confidentiality of their account credentials;
- implementing appropriate local security measures within their own networks;
- ensuring that any systems accessing NetLir's portal or APIs are properly secured and updated.

Clients must **notify NetLir immediately** at **support@netlir.pro** if they suspect unauthorized access, credential compromise, or any security-related issue involving their account.

8. Cookies and Analytics

8.1. Use of Cookies

Our website <https://netlir.pro> uses cookies and similar tracking technologies to ensure proper functionality, security, and improved user experience.

Cookies are small text files stored on your device when you visit a website. They help us recognize your browser, remember your preferences, and analyze how visitors interact with our site.

We use cookies **only where necessary and proportionate** in accordance with the **UK GDPR** and **Privacy and Electronic Communications Regulations (PECR)**.

8.2. Types of Cookies We Use

1. Strictly Necessary Cookies

These cookies are essential for the operation of our website and portal. They enable core features such as login authentication, secure navigation, and access to protected areas.

These cookies do not require user consent and cannot be disabled through our cookie banner.

2. Functional Cookies

These cookies allow the site to remember user choices and preferences — for example, language settings, session persistence, or form completion.

They improve the overall user experience but are optional. You may disable them through your browser without affecting essential functions.

3. Analytics and Performance Cookies

We use privacy-compliant analytics tools (such as **Matomo** or **Google Analytics with IP anonymization**) to collect aggregate data about how visitors use our website.

This helps us understand traffic patterns, optimize content, and improve service reliability.

Analytics cookies never collect personally identifiable information and operate only with anonymized or pseudonymized data.

4. Security Cookies

These cookies support our infrastructure security — for example, detecting unusual login activity or preventing session hijacking.

They are limited to internal operational use and expire automatically after a short period.

8.3. Cookie Consent

When you visit our website for the first time, you will be presented with a **cookie consent banner** explaining our use of cookies.

You can choose to:

- accept all cookies;
- decline optional (non-essential) cookies; or
- customize your cookie preferences.

Your choice will be stored and can be modified at any time by revisiting the cookie settings or clearing your browser cache.

8.4. Managing Cookies

You can control, restrict, or disable cookies through your browser settings at any time. Please note that disabling certain cookies may affect the functionality or usability of our website, particularly the client login portal and secure payment pages.

For more information on managing cookies, visit:

- <https://www.aboutcookies.org>

8.5. Third-Party Cookies

NetLir does not use third-party advertising cookies.

However, embedded tools or integrations (such as payment gateways or analytics platforms) may use cookies in accordance with their own privacy policies.

We recommend reviewing those policies to understand how your data is handled by such third parties.

8.6. Updates to Cookie Practices

We may periodically review and update our cookie practices to reflect changes in technology or regulatory guidance.

The latest version of this section will always be available in this Policy, with the date of last update indicated at the top.

9. Your Data Protection Rights

Under the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, you have several rights concerning the processing of your personal data.

NetLir LTD is committed to ensuring that these rights are respected and that all related requests are handled fairly, transparently, and without undue delay.

9.1. Your Individual Rights

You have the following rights under the UK GDPR:

- **Right of Access (Article 15):**
You may request confirmation of whether we process your personal data and obtain a copy of that data, along with information about how and why it is processed.
- **Right to Rectification (Article 16):**
You may request correction of inaccurate or incomplete personal data held by NetLir. Where possible, we will verify and update the information within our systems and RIPE NCC records.
- **Right to Erasure (“Right to be Forgotten”, Article 17):**
You may request deletion of your personal data where it is no longer necessary for the purposes for which it was collected, or if you withdraw consent (where applicable). However, this right may not apply where retention is required by law, regulatory obligations, or RIPE NCC policy compliance.

- **Right to Restriction of Processing (Article 18):**
You may request that we temporarily suspend the processing of your data, for example, while the accuracy of data or the legitimacy of processing is being verified.
- **Right to Data Portability (Article 20):**
You have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller, where processing is based on consent or contract and carried out by automated means.
- **Right to Object (Article 21):**
You may object to the processing of your personal data where it is based on legitimate interests or for direct marketing purposes.
We will stop processing unless we demonstrate compelling legitimate grounds that override your interests, rights, and freedoms.
- **Right to Withdraw Consent (Article 7(3)):**
Where processing is based on your consent (for example, marketing communications), you have the right to withdraw it at any time without affecting the lawfulness of prior processing.

9.2. Exercising Your Rights

To exercise any of these rights, please contact our Data Protection Officer (DPO) at: **support@netlir.pro**

We will:

- acknowledge your request within **5 working days**;
- respond to verified requests within **30 days** of receipt;
- extend the response period by up to **two additional months** if the request is complex or involves multiple data subjects, notifying you accordingly.

Before processing your request, we may ask for **identity verification** to ensure that personal data is not disclosed to unauthorized persons.

9.3. Limitations and Exceptions

Certain rights may be limited or restricted where:

- processing is required to comply with legal or contractual obligations;
- data must be retained for RIPE NCC audits or network compliance;
- disclosure could adversely affect the rights or freedoms of others;
- data forms part of ongoing legal or regulatory proceedings.

Where such limitations apply, NetLir will provide a clear explanation of the reason for refusal or partial compliance.

9.4. Complaints

If you believe that your data protection rights have been violated, you have the right to lodge a complaint with the **Information Commissioner's Office (ICO)**, the UK's supervisory authority for data protection:

<https://ico.org.uk/>

You may also contact your local supervisory authority if you are located within the European Economic Area (EEA).

10. Data Breach Notification

10.1. Definition of a Personal Data Breach

A **personal data breach** means any security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed by NetLir LTD.

Such incidents may include, but are not limited to:

- unauthorized access to customer accounts or systems;
- loss or theft of storage devices or credentials;
- malware or ransomware attacks compromising stored data;
- accidental disclosure of personal information to third parties.

10.2. Immediate Response

Upon detection or notification of a potential data breach, NetLir will:

1. **Initiate an internal incident response procedure**, led by the Data Protection Officer (DPO) and IT Security team;
2. **Contain and mitigate the impact** of the breach by securing affected systems and isolating compromised resources;
3. **Assess the nature, scope, and severity** of the incident to determine whether personal data has been affected and the potential consequences for individuals.

10.3. Regulatory Notification

If the breach is likely to result in a **risk to the rights and freedoms of natural persons**, NetLir will:

- **notify the Information Commissioner's Office (ICO)** without undue delay and, where feasible, **within 72 hours** after becoming aware of the incident;
- provide the ICO with all required information, including:
 - o nature of the breach;
 - o categories and approximate number of data subjects and records affected;
 - o likely consequences of the breach; and
 - o measures taken or proposed to address it.

If notification is not made within 72 hours, the reason for delay will be documented and communicated to the ICO.

10.4. Notification to Data Subjects

Where a breach is likely to result in a **high risk** to the rights and freedoms of individuals, NetLir will **promptly inform affected clients or individuals**, in clear and plain language, including:

- a description of the nature of the breach;
- likely consequences and potential risks;
- recommended steps the individual should take to protect themselves (e.g., password reset); and
- contact details of the Data Protection Officer for further assistance.

Notification to individuals may be delayed, limited, or omitted where permitted by law — for example, if immediate disclosure would obstruct a criminal investigation or jeopardize system security.

10.5. Record-Keeping and Review

All data breaches, whether notifiable or not, are recorded in the **NetLir Incident Register**, which includes details of the cause, impact, actions taken, and lessons learned. Following each incident, NetLir conducts a **post-incident review** to identify and implement preventive measures and strengthen system resilience.

10.6. Contact for Data Breach Queries

For any questions or concerns about data breaches, please contact:
support@netlir.pro
+44 20 8159 8921

11. Third-Party Links

11.1. External Websites and Services

Our website <https://netlir.pro> may contain links to third-party websites, online tools, or platforms that are not operated or controlled by **NetLir LTD**. These may include:

- external documentation sources (e.g., RIPE NCC, IANA, or compliance registries);
- integrated payment gateways or verification providers;
- communication or analytics services;
- partner or reference pages.

These links are provided **for informational and convenience purposes only**. NetLir does not endorse, monitor, or assume responsibility for the content, accuracy, or practices of such external websites.

11.2. Independent Privacy Practices

Once you leave the NetLir website or customer portal and visit an external platform, the collection, storage, and use of your personal data are governed by that website's own **Privacy Policy** and **Terms of Use**.

NetLir has **no control** over how third parties manage your data, cookies, or tracking technologies, and we cannot guarantee the same level of security or compliance.

We strongly encourage users to:

- review the **privacy policies and cookie notices** of each external website before submitting any personal data;
- exercise caution when interacting with third-party services or providing sensitive information through non-NetLir channels.

11.3. Third-Party Integrations and Processors

Where NetLir integrates with external systems (such as RIPE NCC platforms, payment processors, or infrastructure providers), we ensure that:

- such third parties are **contractually bound** to process data in compliance with **UK GDPR**;
- data shared with them is **limited to the minimum necessary** for performing the intended service; and
- appropriate **Data Processing Agreements (DPAs)** and **security safeguards** are in place.

11.4. Disclaimer

NetLir is not responsible for:

- the security or privacy practices of third-party websites;
- any damages or losses arising from the use of external links; or
- the accuracy or legality of external content.

Your interaction with any external website is entirely at your own risk.

12. Children's Privacy

12.1. Intended Audience

NetLir LTD provides services exclusively to **business, institutional, and professional clients**.

Our offerings — including IP leasing, RIPE NCC sponsorship, and LIR management — are designed for organizations and individuals engaged in lawful commercial or technical activities.

They are **not directed toward minors or consumers under the age of 18**.

12.2. No Intentional Data Collection

NetLir does **not knowingly collect, store, or process personal data** belonging to individuals under 18 years of age.

We do not target, advertise, or market our services to children and do not permit account registration or service activation by minors.

If we become aware that personal information from a child under 18 has been collected inadvertently, we will:

1. promptly investigate the circumstances;
2. **delete or anonymize** such data without undue delay; and

3. take reasonable steps to prevent any further processing.

12.3. Parental and Guardian Requests

If a parent or legal guardian believes that their child's personal data has been provided to NetLir without consent, they are encouraged to contact us immediately at support@netlir.pro. We will take appropriate steps to verify the request and remove any data that should not have been collected.

12.4. Legal Compliance

This section aligns with:

- **Article 8 of the UK GDPR** (conditions applicable to children's consent in relation to information society services); and
- guidance issued by the **Information Commissioner's Office (ICO)** regarding age-appropriate design and children's data protection principles.

NetLir fully supports these principles and ensures that no personal data belonging to minors is used in any operational, analytical, or marketing process.

13. Contact Information

13.1. How to Contact Us

If you have any questions, concerns, or requests regarding this **Privacy Policy**, the way your personal data is handled, or your rights under applicable data protection laws, please contact our **Data Protection Officer (DPO)**:

Data Protection Officer (DPO)

NetLir LTD

71–75 Shelton Street, Covent Garden
London, WC2H 9JQ, United Kingdom

support@netlir.pro

+44 20 8159 8921

We aim to respond to all verified inquiries within **30 calendar days**.

Where necessary, we may request additional information to confirm your identity before processing your request.

13.2. Supervisory Authority

If you believe that your data protection rights have been violated or that we have not adequately addressed your concern, you have the right to file a complaint with the **Information Commissioner's Office (ICO)** — the supervisory authority for data protection in the United Kingdom.

Information Commissioner's Office (ICO)

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom

<https://ico.org.uk/>
+44 (0)303 123 1113

You may also lodge a complaint with your local data protection authority if you reside within the **European Economic Area (EEA)** or outside the UK.

13.3. Updates to This Policy

NetLir reserves the right to review and update this Privacy Policy periodically to reflect changes in legal requirements, business practices, or technology.

The latest version will always be available at <https://netlir.pro/privacy>, and the effective date will coincide with the publication date unless stated otherwise.

By continuing to use our website or services after any update, you acknowledge and agree to the revised terms of this Policy.