

GDPR Policy

This policy explains the core principles governing the processing of personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 for APINAME LTD operating under the “Domain Name API” brand and its resellers.

The UK GDPR is the version of the General Data Protection Regulation applied in the United Kingdom. It is legislation designed to protect the privacy and personal data of individuals in the UK. Its purpose is to regulate data protection uniformly across the UK, give individuals more control over their data, and set clear rules for how data controllers may use personal data.

Additionally, the UK GDPR and the Data Protection Act 2018 ensure the free movement of personal data within the UK, and they set special conditions for transfers of personal data outside the UK.

Below is a summary of how we process personal data from the perspective of resellers, who the parties involved are, and what their roles are.

General Framework for Domain Name API Resellers

For resellers of Domain Name API products and services, regardless of whether the end customer is located in the UK or not, the requirements stemming from the UK GDPR apply to all reseller accounts. APINAME LTD has committed to applying a unified standard of privacy and data protection across its entire platform.

Therefore, all resellers must:

- Read and understand the requirements of the UK GDPR,
- Review policy and contract amendments,
- Implement the required obligations into their business processes.

Failure to do so may expose resellers to significant administrative fines and enforcement actions in their respective jurisdictions.

Domain Name API largely undertakes the technical and contractual compliance on its side; however, especially with respect to customer-facing disclosure texts, cookie notices, privacy notices, explicit consent mechanisms and contract texts — the reseller's responsibility remains.

Please note that if the reseller is located outside the UK but provides services to individuals in the UK, the reseller may be subject to the UK GDPR requirement to appoint a representative in the UK.

Domain Name API – APINAME LTD's UK GDPR Compliance

APINAME LTD, operating under the Domain Name API brand, is committed to protecting personal data in accordance with the UK GDPR and the Data Protection Act 2018. We respect the personal data of our customers and visitors and process it only for lawful, transparent, and legitimate purposes.

Below is a summary of key principles from the UK GDPR that we also adhere to:



- **Lawfulness, Fairness & Transparency:** Personal data is processed lawfully, fairly and in a transparent manner. Data subjects are given as clear and intelligible information as possible.
- **Purpose Limitation:** Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. We only process data where necessary for the initial purpose; if the purpose changes, we assess the legal basis before re-using the data.
- **Data Minimisation:** We collect only personal data that is necessary for the purpose. We avoid collecting unnecessary personal data. This approach strengthens data security and eases legal compliance.
- **Accuracy:** Personal data is maintained accurately and, where necessary, kept up to date. We review and rectify or erase inaccurate or outdated data without undue delay. Our customers and resellers are obliged under our Terms of Use to keep their information accurate.
- **Storage Limitation:** Personal data is not kept in an identifiable form longer than necessary for the purpose. When the processing purpose ends or the legal retention period expires, data is erased or anonymised.
- **Integrity & Confidentiality (Security):** Personal data is protected by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage. Our system architecture is layered, and we use encryption, access controls and audit logs where possible. Only authorised personnel with a legitimate business need may access personal data. In the event of a personal data breach, we follow the notification procedures required by the UK GDPR and the Data Protection Act 2018, informing data subjects and, if required, the UK Information Commissioner's Office (ICO) within the legally required timeframe.

Data Subject Rights (UK GDPR)

Under the UK GDPR, data subjects have the right to:

- Access their personal data (Article 15),
- Rectify inaccurate personal data (Article 16),
- Erase personal data ("right to be forgotten") (Article 17),
- Restrict processing (Article 18),
- Data portability (Article 20),
- Object to processing (Article 21).

A data subject also has the right to lodge a complaint with the UK Information Commissioner's Office (ICO) regarding the processing of their personal data by APINAME LTD.

Controller, Processor and Reseller Roles

Under the UK GDPR:

- **APINAME LTD / Domain Name API** is the data controller with respect to:



- Managing your reseller account,
- Billing,
- Reseller support,
- Providing domain registration services.
- **Registry operators (and ICANN)** may be considered as joint controllers in respect of domain registration data for certain TLDs.
- **The Reseller** collects domain registration data from the end user and passes it to Domain Name API; to the extent the reseller acts on behalf of Domain Name API, the reseller acts as a data processor.
 - Therefore, the reseller must accept the “Reseller Data Processing Agreement” provided by Domain Name API and must use data-protection compliant contracts with end customers.

Which Data is Collected?

The types of data collected vary depending on the TLD registry and ICANN requirements; at minimum it includes:

- Domain name,
- Nameserver details,
- Registrant name,
- Registrant company name (if any),
- Registrant address (street, city, postal code, country),
- Registrant telephone number and email address.

3

Additionally, for managing your reseller account:

- Account owner name,
- Account owner company name,
- Billing/account address,
- Contact information (telephone, email),
- Payment and invoice data,

which is processed under the legal basis of contract performance (UK GDPR Article 6(1)(b)).

Domain Registration Process and Legal Basis

During domain registration:

- The legal basis for collecting data and processing by Domain Name API is largely performance of a contract (Article 6(1)(b) UK GDPR).
- Transfer of data to registries is based on:



- Either contract performance (Article 6(1)(b)), or
- Legitimate interests (Article 6(1)(f)) such as ownership verification, dispute resolution, security monitoring, and abuse prevention.

Data Retention

Personal data is erased or anonymised without undue delay when the processing purpose ceases or the legal retention period expires. Domain registration data may be retained in accordance with ICANN and registry requirements for a defined period (e.g., at least 2 years after domain expiry).

Under UK GDPR Articles 17 and 18:

- A data subject may request erasure, or
- Restrict processing. However, due to legal retention obligations or contractual requirements with ICANN/registries, not all requests may result in immediate erasure.

International Data Transfers (Outside the UK)

If personal data is transferred outside the UK, such transfers are compliant with UK GDPR's international transfer rules, for example:

- Transfers to countries deemed adequate by the UK,
- Or transfers protected by a UK-approved International Data Transfer Agreement (IDTA) or a UK Addendum to the EU Standard Contractual Clauses. If resellers conduct international transfers (e.g., via their infrastructure or sub-processors), they must ensure legal bases and contractual safeguards compliant with UK GDPR.

4

Domain Disputes & UDRP/URS

All gTLD registrations are subject to ICANN policies such as the Uniform Domain-Name Dispute Resolution Policy (UDRP) and Uniform Rapid Suspension (URS). During these procedures:

- Registrant data may be passed to the dispute resolution provider and the complainant. Such disclosures are justified under Article 6(1)(b) UK GDPR as performance of the registration contract and under relevant ICANN policies.

Disclosure and Privacy of Registration Data

Who and how registration data will be disclosed is determined by the relevant registry policies and applicable law.

- For many gTLDs, much of the registrant's personal data will not be directly published in WHOIS; often only limited data such as country and region/state appear.
- Additional data may only be disclosed when:
 - There is consent (opt-in), or
 - Legal obligation (Article 6(1)(c)), or



- Contract / ICANN policy (Article 6(1)(b)), or
- Legitimate interests (Article 6(1)(f)).
A web form may be provided for communication with the registrant without directly publishing their email address.

