Technical and Organisational Measures

IDDQD Limited (Ideal Postcodes)

This document describes the technical and organisational measures implemented by IDDQD Limited ("Ideal Postcodes") to protect Personal Data processed on behalf of its clients, in accordance with Section 7.1 of its Data Processing Agreement.

IdealPostcodes

1. Organisational Measures

1.1 Information Security Certification

Ideal Postcodes holds **ISO 27001 certification**, the internationally recognised standard for information security management systems. This certification covers the design, development and operation of the Ideal Postcodes service.

1.2 Policies & Governance

Ideal Postcodes maintains a suite of information security and data protection policies under its ISO 27001 framework, including an Information Security Policy, Data Protection Policy (aligned with UK GDPR and the Data Protection Act 2018), Data Retention and Disposal Policy, and a Data Breach Response and Incident Management Procedure.

1.3 Staff Training & Awareness

All staff handling Personal Data receive data protection training. Staff are subject to contractual confidentiality obligations as a condition of employment.

1.4 Supplier & Subprocessor Management

Due diligence is conducted on all subprocessors prior to appointment. Written data processing agreements are in place with all subprocessors. A current list of subprocessors is publicly maintained and updated at:
https://terms.ideal-postcodes.co.uk/data-processing/data-processors.html

Clients are notified of new subprocessors at least one calendar month before they commence processing, with a 14-day written objection window.

1.5 Risk Management

Risk management is conducted under the ISO 27001 framework. Data Protection Impact Assessments (DPIAs) are conducted for high-risk processing activities.

2. Technical Measures

2.1 Access Controls

Access to systems containing Personal Data is restricted on a need-to-know basis. Role-based access controls (RBAC) are in place, with different staff roles having different levels of access to systems and infrastructure. Multi-factor authentication (MFA) is required for all developer and administrator access to cloud infrastructure and internal tools. API Keys are issued per client and can be individually restricted, rotated or revoked via the client dashboard at any time. Leavers' access is revoked as part of a formal offboarding procedure.

2.2 Encryption

All data in transit is encrypted — the Ideal Postcodes API is only accessible over HTTPS (TLS), enforced across all endpoints. Data at rest is encrypted using AES-256, enforced via cloud provider infrastructure.

2.3 Network & Infrastructure Security

Ideal Postcodes operates across multiple cloud providers with infrastructure hosted across UK, EU, and US regions. US-based infrastructure serves API traffic originating from the US; any logs and usage data are forwarded to the EU for storage. **All Personally Identifiable Information (PII) is stored and processed exclusively within the EU.** No PII is transferred to or stored within US-based infrastructure. Infrastructure security is managed under the ISO 27001 framework. Service uptime and availability is monitored continuously and publicly reported at: https://status.ideal-postcodes.co.uk

2.4 Application Security

Ideal Postcodes follows secure development practices. Independent penetration testing is conducted annually by a qualified third party. Software libraries are open source and publicly auditable via GitHub at https://github.com/ideal-postcodes. Clients are provided with comprehensive documentation on secure API integration practices, including API key management, URL allowlisting and rate limiting.

2.5 Monitoring & Logging

API usage is logged per key. Clients can query their own usage statistics and lookup logs via the API. Automated alerts are sent when 90% and 100% of daily lookup caps are reached. Per-IP address rate limiting is available to detect and mitigate abusive usage patterns. Server logs are retained for 28 days. Address query data is redacted after 21 days by default; this retention period is configurable by the client and can be disabled entirely.

2.6 Business Continuity & Disaster Recovery

A formal Business Continuity Plan (BCP) is in place. IDDQD's fully remote, multi-cloud architecture means the business is not susceptible to single-location failures such as power outages, natural disasters or physical infrastructure loss. The BCP is triggered at Severity 1 incidents, including confirmed or suspected data breaches, or where incident recovery timelines cannot be met. Service continuity is supported by SLAs with cloud hosting providers across multiple regions.

2.7 Personal Data Minimisation

Only the minimum Personal Data necessary to provide the Service is processed. Address query data is stored separately from client account information. Address queries not linked to identifiable individuals are not treated as Personal Data. IDDQD does not use address query data for direct marketing or to identify individual users.

3. Physical Security

IDDQD operates as a fully remote company with no on-premise data infrastructure. Physical security of underlying infrastructure is managed by cloud hosting providers, all of whom maintain their own security certifications and controls. IDDQD's physical security obligations under ISO 27001 apply to staff devices and remote working environments.

4. Incident Response & Breach Notification

A documented incident response procedure is in place under the ISO 27001 framework. In the event of a Personal Data breach, IDDQD will notify the affected client without undue delay. IDDQD will cooperate with the client to investigate, mitigate and remediate any breach. Where required, breaches are reported to the ICO within 72 hours in accordance with UK GDPR Article 33. IDDQD will provide reasonable assistance to clients with DPIAs and prior consultations with supervisory authorities.

5. Data Retention & Deletion

Address query data is redacted after 21 days by default. Clients can configure this retention period or disable storage of query data entirely via their dashboard. Upon termination of the data processing relationship, IDDQD will delete or return Personal Data in accordance with the client's instructions and the terms of the Data Processing Agreement. Client account data is retained only as long as necessary to fulfil contractual and legal obligations.

6. Certifications

Certification / Standard	Status
ISO 27001	Certified
PCI DSS	Not applicable — no card data processed

7. Infrastructure Summary

Item	Detail
Hosting model	Multiple cloud providers
Infrastructure regions	UK, EU, US (East and West)
PII data residency	EU only
API endpoint	https://api.ideal-postcodes.co.uk
Service status	https://status.ideal-postcodes.co.uk
Subprocessor list	https://terms.ideal-postcodes.co.uk/data-processing/data-processors.html
Open source libraries	https://github.com/ideal-postcodes

8. Client-Side Security Controls

Ideal Postcodes provides clients with the following technical controls to manage and secure their own use of the service:

- **URL Allowlisting**
  API Key requests can be restricted to specific domains and protocols

- **Daily Lookup Caps**
  A configurable hard daily cap per API Key, with automated alerts at 90% and 100% usage

- **Per-IP Rate Limiting**
  Individual IP addresses can be limited to a set number of daily lookups

- **Backend Integration Guidance**
  Clients are advised to use server-side integrations for sensitive environments to prevent API Key exposure in client-side code

- **Key Rotation & Revocation**
  API Keys can be rotated or revoked instantly via the client dashboard

Full documentation: https://docs.ideal-postcodes.co.uk/docs/guides/api-key-secure