# Auko Ltd - Privacy Policy

## 1. Introduction

Auko Ltd (“Auko”, “we”, “us”, “our”) is committed to protecting the privacy and security of personal data. This Privacy Notice explains how we collect, use, disclose, store, and protect personal data when individuals interact with our website, products, and services, including the DrawCheck application.

This Notice is designed to provide transparency in accordance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**. It applies to:

- Visitors to our website
- Users of the DrawCheck application
- Representatives of customer organisations
- Suppliers, contractors, and other business contacts
- Individuals who communicate or engage with us in a commercial context

Auko acts as either a **Data Controller** or a **Data Processor** depending on the specific processing activity:

- We act as a **Data Controller** when we determine the purpose and means of processing (e.g., account management, billing, website operations, marketing communications).

- We act as a **Data Processor** when we process data on behalf of a customer, primarily when analysing customer-uploaded drawings, documents, or standards in the DrawCheck application.

This Notice explains:

- What personal data we collect
- How and why we process it
- Our legal bases for processing
- How long we keep it
- How we share it
- The measures we take to keep it secure
- The rights available to individuals
- How to contact us with questions or concerns

If you have any questions about this Notice or your personal data, you can contact us at: privacy@auko.ai

# 2. About Auko Ltd

Auko Ltd (“Auko”) is a UK-registered technology company that develops AI-powered tools to support engineering design, analysis, and product development. Our primary product, DrawCheck, provides automated review and analysis of engineering drawings and related technical documentation.

## 2.1 Company Identity

**Auko Ltd**
51 Church Lane
Sevenhampton, Cheltenham
GL54 5SW, UK

Company Number: 16595090

Auko is the **Data Controller** for most personal data processed through our website, platform account management, communications, and business operations.
Auko is the **Data Processor** when handling customer-provided documents or content within DrawCheck.

## 2.2 Contact for Data Protection Matters

For any questions, requests, or concerns relating to this Privacy Notice or your personal data, you can contact us at:

**Email:** privacy@auko.ai
**Address:**
51 Church Lane
Sevenhampton, Cheltenham
GL54 5SW, UK
**Attention:** Data Protection Lead

## 2.3 Data Protection Lead

Auko’s **Data Protection Lead** (DPL) is the **Chief Technology Officer (CTO)**. The DPL oversees compliance with this Privacy Notice and applicable data protection laws and acts as a contact point for queries relating to the handling of personal data.

## 2.4 Definitions

For clarity and consistency, key terms used in this Notice have the following meanings:

- **“Personal Data”** – Any information relating to an identified or identifiable individual.
- **“Special Category Data”** – Sensitive personal data requiring additional protection under UK GDPR (e.g., health, ethnicity, biometrics).

- **“Processing”** – Any operation performed on personal data, including collection, storage, use, transmission, or deletion.
- **“Data Controller”** – The organisation that determines the purposes and means of processing personal data.
- **“Data Processor”** – An organisation that processes personal data on behalf of a controller.
- **“Customer”** – An organisation purchasing or using Auko’s services.
- **“User”** – An individual accessing Auko’s website or applications, whether on their own behalf or as a representative of a customer.
- **“DrawCheck Content”** – Engineering drawings, documents, standards, or other files uploaded by customers to be processed through the DrawCheck application.

# 3. Personal Data We Collect

Auko Ltd collects and processes personal data in several categories depending on how individuals interact with our website, services, and applications. We collect only the minimum personal data necessary to deliver our services, operate our business, and meet our legal obligations.

Personal data is grouped into the categories below for clarity.

## 3.1 Account and Identity Data

Information required to create and administer user accounts, including:

- Name
- Email address
- Job title or role
- Company or organisation name
- Authentication credentials (hashed—never stored in plain text)
- Access roles and permissions
- Account configuration settings

**Source:** provided directly by users or their employer.

## 3.2 Contact and Communication Data

Information used to manage our relationship with customers and respond to enquiries, including:

- Email correspondence
- Support tickets and chat interactions
- Call summaries or meeting notes (where applicable)
- Preferences for receiving communications
- Records of interactions with our support team

**Source:** provided directly by users or captured during communications.

### 3.3 Customer-Submitted Drawings, Standards, and Files (“DrawCheck Content”)

These are documents uploaded to the DrawCheck application for processing. They may include:

- Engineering drawings (2D/3D formats)
- Customer-specific standards and rule sets
- Technical documentation or specifications
- Model inputs used for analysis
- Metadata associated with files

DrawCheck Content may **incidentally contain personal data**, such as:

- Names appearing in title blocks
- Sign-off initials
- Author identifiers

Auko **does not extract, analyse, enrich, classify, or store** this incidental personal data beyond what is necessary to process the file.

**Source:** provided directly by customer users.

### 3.4 Technical and Usage Data

Collected automatically when users interact with our website or application:

- IP address and approximate geolocation
- Browser type, device type, operating system
- Access timestamps
- Session identifiers
- Application performance metrics
- API usage events
- Error codes and status information
- Authentication and authorisation logs
- Metadata about DrawCheck processing (e.g., file sizes, processing durations)

Auko does **not** log or store customer drawings, standards, or AI model outputs.

**Source:** automatically collected via our systems.

### 3.5 Log and Audit Data

Metadata recorded for security, monitoring, and compliance:

- Authentication attempts (successful and unsuccessful)
- User role changes
- Access control events
- System events related to processing
- High-level diagnostic information
- Security event metadata

These logs do **not** contain customer content or personal data other than identifiers necessary for security auditing.

**Source:** generated by Auko’s infrastructure.

### 3.6 Billing and Transaction Data

For customers who pay for services:

- Company billing details
- Purchase order information
- Subscription records
- Payment confirmations
- Invoices and transaction history

Auko does **not** process or store full payment card details. Payments are handled by a third-party provider acting as a separate data controller or processor.

**Source:** provided by customer finance teams, users, or via our billing provider.

### 3.7 Supplier, Contractor, and Employee Data (High-Level)

For operational and business management purposes, Auko processes limited personal data relating to:

- Employee and contractor identification data
- Contact details
- Contractual documentation
- Operational and access records

Full details of employee data processing are covered in separate internal policies, not in this Notice.

### 3.8 Marketing and Preference Data

When users subscribe for updates or marketing communications:

- Name
- Email
- Communication preferences

- Engagement metrics for emails (open/click rates)

Marketing communications are only sent where **consent** or **legitimate interests** apply.

### 3.9 Sensitive and Special Category Data

Auko does **not** intentionally collect or require special category data for any purpose.

If such data appears incidentally within customer documents, it is handled in accordance with the DrawCheck processing workflow and deleted immediately after processing.

## 4. Special Categories of Data

Under the UK GDPR, certain types of personal data are classified as *Special Category Data*, requiring enhanced protection. These include data relating to health, ethnicity, biometrics, religious beliefs, political opinions, sexual orientation, and similar sensitive attributes.

### 4.1 Auko's Position on Special Category Data

Auko Ltd does **not** intentionally collect, request, or require any Special Category Data for the operation of its website, DrawCheck application, or business services.

We design our systems and workflows such that Special Category Data is highly unlikely to be provided or processed.

### 4.2 Incidental Appearance of Special Category Data in Customer Documents

In rare cases, Special Category Data may **incidentally appear** within engineering drawings or documents uploaded by customers—for example:

- A name or identifier that indirectly reveals sensitive information
- Notes or metadata included in a customer-uploaded file
- Historical annotations embedded within technical documentation

Where this occurs:

- Auko does **not** extract, classify, or analyse such data.
- It is processed **only to the extent strictly necessary** to perform the DrawCheck analysis requested by the customer.
- It is retained **only for the short technical period required** to complete processing.
- It is deleted **immediately after processing**, unless a processing error necessitates temporary retention (up to 24 hours).

Auko's systems do not create or derive any sensitive personal profiles from customer uploads.

### 4.3 Prohibition on Uploading Special Category Data

Customers are explicitly instructed **not** to upload Special Category Data to the DrawCheck service.
This includes embedding sensitive information in:

- Engineering drawings
- Standards
- Specifications
- Supporting documentation

Auko may notify a customer administrator if repeated uploads appear to contain sensitive data.

### 4.4 Safeguards for Incidental Processing

Auko implements the following safeguards:

- Automated deletion of drawings immediately after analysis
- No AI enrichment, classification, or profiling
- No inclusion of sensitive data in logs or monitoring systems
- Strict access controls
- Encryption in transit and at rest
- Processing limited to the region selected by the customer (UK/EU or optional US region)

## 5. How We Obtain Personal Data

Auko Ltd collects personal data from a variety of sources depending on how individuals interact with our website, platform, and services. We obtain personal data only where necessary for defined purposes and only through lawful means.

### 5.1 Personal Data Provided Directly by Users

Most personal data is supplied directly by individuals when they:

- Create or manage an account
- Upload drawings, standards, or other files into DrawCheck
- Contact us with a query or request support
- Participate in onboarding, training, or demonstrations
- Opt in to marketing or updates
- Provide billing or contract information
- Enter into a commercial relationship with Auko

Users and customer organisations control the completeness and accuracy of this data.

## 5.2 Personal Data Provided by Customer Organisations

In a business-to-business context, organisations may provide personal data relating to their staff, such as:

- Names and email addresses of authorised users
- Role and permission assignments
- Billing or administrative contacts
- Project or team documentation containing user identifiers

Where customer organisations act as the Data Controller, Auko processes such data only under their documented instructions.

## 5.3 Personal Data Provided Through Use of the DrawCheck Service

When using DrawCheck, customers may upload documents that contain incidental personal data. This may appear in:

- Title blocks
- Revision histories
- Approval signatures or initials
- Embedded annotations
- Metadata within uploaded files

Auko processes this data only as necessary to perform the requested analysis and deletes it automatically after processing.

## 5.4 Automatically Collected Personal Data

When users interact with our website or application, Auko systems automatically collect limited personal data, including:

- IP address
- Device and browser type
- Usage metadata
- Authentication and authorisation events
- Session identifiers
- Application performance telemetry

This data is necessary for security, fraud prevention, service stability, and performance optimisation.

## 5.5 Personal Data from Third Parties

We may receive personal data from trusted third-party sources, such as:

- Authentication providers (e.g., identity verification or SSO services)

- Billing platforms (company billing details and payment metadata)
- Customer procurement systems
- Communication systems (e.g., support ticketing tools)

These providers may act as independent controllers or processors depending on their role.

### 5.6 Publicly Available Sources

In limited circumstances, Auko may obtain business contact information from publicly available or legitimate commercial sources, such as:

- Company websites
- Professional directories
- Networking platforms
- Public registers (e.g., Companies House)

This data is used only for business-to-business communication and outreach where lawful.

## 6. Purposes and Lawful Bases for Processing

Auko Ltd processes personal data only where we have a lawful basis under the UK GDPR and only for purposes that are explicit, legitimate, and proportionate. This section explains **why** we process personal data, **what data is involved**, **the legal basis for doing so**, and **whether we act as a controller or a processor**.

### 6.1 Summary of Lawful Bases We Rely Upon

Auko uses the following lawful bases depending on the activity:

- **Contract** – necessary to provide our services, maintain accounts, and process uploaded files.
- **Legitimate interests** – necessary for security, product reliability, business operations, supplier management, and limited B2B marketing.
- **Legal obligation** – necessary to comply with tax, accounting, employment, and regulatory requirements.
- **Consent –** used for marketing communications where required.

Auko does **not** rely on legitimate interests for any processing that overrides the rights or freedoms of individuals.

| **Purpose of processing** | **Categories of personal data** | **Lawful Basis** | **Auko Role** | **Retention Summary** |
|---|---|---|---|---|
| Account creation and management | Identity data, contact data, authentication details, role | Contract | Controller | Retained for duration of account + short post-closure period |

| | | | | |
|---|---|---|---|---|
| | assignments | | | |
| Providing the DrawCheck service | DrawCheck Content (files uploaded), incidental personal data, technical metadata | Contract | Processor | Drawings deleted immediately after processing; standards retained until removed by customer |
| Customer support and troubleshooting | Contact data, account data, communication data, technical logs | Contract / Legitimate interests | Controller | Retained for duration of support interaction + short period for audit |
| Security monitoring and fraud prevention | IP address, authentication logs, session metadata, device information | Legitimate interests | Controller | Retained only as necessary for security and audit purposes |
| Service performance, reliability, and diagnostics | Application telemetry, error codes, technical metadata (no customer content) | Legitimate interests | Controller | Minimal; retained only for operations and debugging |
| Billing and financial administration | Billing contacts, company details, transaction records | Contract / Legal obligation | Controller | Retained as required by tax and accounting law |
| Supplier and contractor management | Identity and contact data, contractual documentation | Contract / Legal obligation | Controller | Retained as required for business and legal purposes |
| Business-to-business marketing | Business contact details, email, marketing preferences | Legitimate interests / Consent | Controller | Retained until consent withdrawn or objection raised |
| Compliance with legal obligations | Any data necessary for statutory compliance (e.g., regulatory reporting) | Legal obligation | Controller | Retained as legally required |
| Product demonstrations, onboarding, and evaluations | Identity and contact data, voluntary communications | Legitimate interests / Contract | Controller | Retained for the duration of the evaluation period |
| Platform security investigations | Relevant metadata, audit logs, access events | Legitimate interests | Controller | Retained only as required for investigation and remediation |

### 6.3 Uses of Personal Data That Auko Does Not Perform

To provide absolute clarity, Auko does **not**:

- Use customer-uploaded documents for model training

- Extract or classify personal data from engineering drawings
- Profile individuals
- Conduct automated decision-making that produces legal or significant effects
- Sell or rent personal data
- Share personal data for advertising purposes

### 6.4 Lawful Basis for Incidental Personal Data in Uploaded Files

When personal data appears inside engineering drawings or technical documents uploaded to DrawCheck:

- The lawful basis is **Contract**, because processing is necessary to deliver the service.
- Auko processes this data **only transiently**, solely to perform the requested analysis.
- The data is deleted automatically once processing completes.

This complies with the data minimisation and purpose limitation principles under UK GDPR.

### 6.5 If the Purpose Changes

If Auko wishes to use personal data for a purpose not listed here:

- We will inform affected individuals or customer controllers in advance
- We will identify a new lawful basis
- Processing will not occur without appropriate notice or agreement

## 7. How Customer Files (Drawings, Standards, Documents) Are Processed

DrawCheck allows customers to upload engineering drawings, standards, specifications, and related technical documentation ("DrawCheck Content"). These files may contain proprietary intellectual property and, in rare cases, incidental personal data contained within title blocks, annotations, or document metadata.

Auko treats all DrawCheck Content as **Highly Confidential**, imposing the strongest technical and organisational safeguards.

### 7.1 Auko's Role as a Data Processor

For DrawCheck Content, Auko acts strictly as a **Data Processor**.
This means:

- The customer is the **Data Controller**.
- Auko processes files only according to the customer's instructions.
- Auko does not determine how such data is used beyond delivering the requested analysis.

- Auko does not extract, interpret, or store personal data found incidentally within the files.

A Data Processing Agreement (DPA) applies to this processing where contractually required.

## 7.2 Types of Files Processed

DrawCheck processes:

- 2D engineering drawings (all common formats)
- 3D or technical documentation formats (where supported)
- Customer standards, rule sets, and specification documents
- Associated project files necessary for engineering analysis

These files may contain:

- Proprietary technical IP
- Customer engineering methods and rulebooks
- Version numbers, part identifiers, and design references
- Names, initials, or user identifiers appearing incidentally

Auko does **not** require or request personal data within these files.

## 7.3 Description of the Processing Workflow

The DrawCheck workflow consists of the following controlled steps:

### 7.3.1. File Upload

The user uploads a file securely via the DrawCheck interface or API.
The file is encrypted in transit using TLS 1.3.

### 7.3.2. Temporary Storage for Processing

Uploaded files are placed in a secure, region-specific storage location (UK/EU or optional US region). This storage is strictly access-controlled and segregated from other tenants unless the customer has a dedicated environment.

### 7.3.3. AI and Rules-Based Analysis

The file is processed using:

- Auko’s proprietary retrieval workflows
- Customer-specific rule sets
- Approved AI foundation models offered through AWS Bedrock

Only the minimum necessary file data is sent to the AI components for the purpose of analysis. Auko **never** uses DrawCheck Content to train unless consent is explicitly granted by the customer.

#### 7.3.4. Report Generation

The result is:

- A structured findings report
- A summary of rule matches and violations

AI output is not logged or stored outside the customer's environment except as part of the generated report.

#### 7.3.5. File Deletion

Once analysis is completed:

- **Drawings are deleted immediately**
- In case of a processing failure, temporary retention of the file may occur for **up to 24 hours** solely for error recovery
- Customer standards remain stored only as necessary to support future analyses for that customer

Temporary files are automatically removed through enforced lifecycle policies.

### 7.4 Handling of Incidental Personal Data

Where a file contains incidental personal data (e.g., designer name in a title block):

- Auko does not extract, analyse, or store it
- Such data is only processed transiently to perform the requested analysis
- The data is automatically deleted with the underlying file
- No incidental personal data is included in logs, telemetry, or monitoring systems
- Customer reports may reference part numbers or rule failures but do not include personal identifiers

Auko complies with the principles of data minimisation and storage limitation.

### 7.5 Security Controls Applied to Customer Files

DrawCheck Content is protected using:

- Encryption in transit (TLS 1.3)
- Encryption at rest using industry-standard cloud provider mechanisms
- Strictly limited access (CTO only by default, with controlled escalation)
- Region-specific data processing (UK/EU or optional US region)
- Isolated environments for enterprise tenants upon request

- Zero persistent logging of customer content
- Automated deletion enforced by storage lifecycle policies
- Serverless architecture reducing attack surface
- No extraction of sensitive personal data
- No model training or dataset enrichment using customer files

These controls align with UK GDPR expectations, NCSC Cloud Security Principles, and industry best practices for protecting sensitive engineering IP.

## 7.6 Customer Control of Data

Customers maintain control over:

- Which files are uploaded
- The standards used for evaluation
- Who within their organisation can upload or access content
- When retained standards or reports are deleted
- Whether they use multi-tenant or fully isolated deployments
- Which hosting region their environment uses

Auko processes DrawCheck Content solely under customer direction.

## 7.7 Prohibited Uses of Customer Files

Auko does **not**:

- Use any customer files for AI model training
- Use customer content for product improvement beyond aggregate metadata
- Analyse or infer personal data
- Share customer files with third parties except trusted infrastructure providers under strict contractual controls
- Store customer content outside the region selected by the customer
- Access customer content for any purpose other than providing the service and ensuring its security
- Allow files to be used in demo, training, or test environments

## 7.8 Customer Requests for Deletion

Auko allows:

- Immediate customer-initiated deletion of standards and stored configurations
- Deletion of generated reports upon request
- Permanent deletion of all customer data within 30 days following account closure
- Earlier deletion where legally or contractually required

Auko supports demonstration of deletion (upon request) for compliance audits.

# 8. Automated Decision-Making and AI Usage

Auko Ltd uses artificial intelligence (AI) and automated analysis techniques within the DrawCheck application to support engineering drawing review. This section explains how AI is used, the safeguards applied, and the limitations of such processing.

Auko is committed to transparency and ensures that AI is used responsibly, securely, and in accordance with UK GDPR.

## 8.1 No Automated Decision-Making Affecting Individuals

Auko does **not** use AI systems to make automated decisions that produce legal or similarly significant effects on individuals under Article 22 of the UK GDPR.
DrawCheck analyses engineering data, not personal data. The outputs:

- Do not evaluate individuals
- Do not profile human behaviour
- Do not determine eligibility, access, or rights
- Have no personal consequences for identifiable individuals

DrawCheck's AI processing is limited to **technical document analysis**.

## 8.2 Purpose of AI in DrawCheck

AI is used solely to:

- Interpret engineering drawings
- Match documents against customer standards
- Generate structured technical findings
- Assist with pattern recognition, compliance checks, and rule evaluation
- Improve precision of engineering analysis workflows (not personal data processing)

## 8.3 No Personal Data Used for Model Training

Auko does **not** use customer data—including engineering drawings, standards, or incidental personal data—for:

- Training AI models
- Fine-tuning models
- Model evaluation
- Dataset creation
- Benchmarking
- Product improvement outside statistical metadata

Customer content is not retained in any AI model or dataset used by Auko or third-party AI providers.

## 8.4 How AI Models Are Used

Auko uses AI capabilities provided through **AWS Bedrock**, including models developed by Anthropic and other approved vendors. AI requests operate under the following constraints:

- Only the **minimum required** portion of uploaded files is used to generate technical analysis.
- Content is transmitted and processed **within the customer's chosen region** (UK/EU or optionally US).
- Processing occurs entirely inside AWS-managed, enterprise-grade environments.
- Providers do **not** retain or use customer data for model training.

These assurances are derived from AWS Bedrock's contractual and technical design.

## 8.5 Prompt Construction and Data Inputs

Inputs to AI systems may include:

- Extracted technical snippets from uploaded drawings
- Customer-defined engineering standards
- Non-personal metadata
- System-generated technical queries

Customer content is always:

- Transient
- Secured
- Limited in scope
- Deleted after processing
- Excluded from logs
- Not visible to any party other than Auko and the AI model provider authorised by the customer's environment

Personal data is not deliberately included and is ignored if present.

## 8.6 Outputs and Reports

AI output is:

- Incorporated into the customer's DrawCheck report
- Stored only as needed to provide the service
- Not used to train or improve models
- Not shared with third parties except infrastructure providers under strict contractual safeguards

Output does **not** include any extracted personal information from the source files.

## 8.7 Human Oversight and Control

Auko maintains human-in-the-loop oversight for AI system design, deployment, and monitoring. This includes:

- Manual code review of AI pipeline logic
- Monitoring of AI system behaviour
- Auditable logs (metadata only)
- Controls preventing unintended retention of customer content
- CTO oversight for AI system changes

Customers maintain full control of uploaded files and resulting reports.

## 8.8 AI Safety and Ethical Restrictions

Auko adheres to the following AI safety commitments:

- No model training on customer data
- No profiling or inference about individuals
- No extraction of personal identifiers
- No high-risk AI uses (e.g., biometrics, surveillance, behavioural analysis)
- No transfer of customer content outside permitted regions
- No exposure of customer content to non-approved AI systems

AI processing is limited entirely to technical engineering analysis.

# 9. Data Retention

Auko Ltd retains personal data only for as long as necessary to fulfil the purposes for which it was collected, to meet contractual or legal requirements, or to support legitimate operational needs. Retention periods vary according to the category of data, the nature of the processing, and the role Auko performs (controller or processor).

Auko applies the principles of data minimisation and storage limitation throughout its operations.

## 9.1 Retention of DrawCheck Content (Processor Role)

### Customer-Uploaded Drawings

- Deleted immediately once processing is successfully completed.
- If processing fails, drawings may be retained for up to 24 hours solely to allow retries and error resolution.
- Drawings are never retained longer than strictly necessary and are not backed up.

### Customer Standards and Rule Sets

- Retained for the duration of the customer account to allow repeated analyses.
- Can be deleted at any time by the customer through the application or by written request.
- Permanently deleted within 30 days following account closure.

### Generated Reports

- Retained for the duration of the customer relationship unless the customer deletes them earlier.
- Deleted within 30 days of account closure unless a shorter period is requested.

Auko does not store personal data from DrawCheck Content in logs, monitoring tools, or analytics systems.

## 9.2 Retention of Account and User Data (Controller Role)

### User Profiles and Authentication Records

- Retained for the duration of the account.
- Deleted or anonymised shortly after account closure, typically within 30 days.

### Role Assignments and Permission Records

- Retained for the duration of the account.
- May be retained for a limited time afterward for security and audit purposes.

### Business Contact Information

- Retained for the duration of the commercial relationship.
- Retained for up to six years afterward where necessary for contract management, audit, or dispute resolution.

## 9.3 Retention of Communication and Support Data

### Support Tickets and Correspondence

- Retained for the duration of the support engagement.
- Archived for up to two years for audit, training, and service quality assurance unless earlier deletion is requested.

### Customer Feedback and Feature Requests are

- Retained for as long as relevant to product development or until the customer requests removal.

## 9.4 Retention of Technical, Security, and Monitoring Data

### Logs and Audit Trails

- Contain metadata only.
- Retained only as long as necessary for security, operational stability, and fraud prevention.
- Typical retention: 30–180 days depending on log type.
- Certain security logs may be retained longer where required for investigation.

### Telemetry and Performance Metrics

- Contain no customer content.
- Retained only for operational analytics and system optimisation.
- Typically retained for 30–90 days.

### Authentication Metadata

- Retained for security audit and compliance purposes.
- Typically retained for 90 days, subject to extension for investigations.

## 9.5 Retention of Billing and Financial Data

### Bills, Invoices, and Transaction Records

- Retained for six years in accordance with tax and accounting requirements.
- Includes invoice metadata and billing contact details.

### Payment Method Information

- No payment card data is stored by Auko.
- Payment metadata retained by the billing provider according to their retention schedule.

## 9.6 Retention of HR, Contractor, and Supplier Data

### Employment and Contractor Records

- Retained in accordance with statutory requirements (typically up to six years after termination).
- Access is strictly limited.

### Supplier Contact Information and Contracts

- Retained for the duration of the supplier relationship.
- Retained for up to six years afterward for business and legal continuity.

## 9.7 Retention Following Account Closure

When a customer terminates their account:

- Drawings are already deleted immediately after processing.
- Customer standards and reports are deleted within 30 days unless earlier removal is requested.
- Account data is deleted or anonymised shortly after closure, typically within 30 days.
- Logs, billing records, and legally mandated information may be retained for statutory periods.

Customers may request expedited deletion at any time where legally permissible.

### 9.8 Exceptions and Legal Requirements

Auko may retain certain limited data for longer where:

- Required by law or regulatory obligations.
- Necessary for the establishment, exercise, or defence of legal claims.
- Required for financial auditing, tax obligations, or fraud prevention.
- A legal hold or investigation is in progress.

Such retention is strictly limited to what is necessary and proportionate.

### 9.9 Anonymisation

Where appropriate, personal data may be anonymised instead of deleted. Anonymised data is no longer considered personal data and may be retained indefinitely for statistical, analytical, or service improvement purposes that do not involve personal information.

## 10. Sharing Your Personal Data

Auko Ltd shares personal data only where necessary to operate our services, fulfil contractual or legal obligations, or support the security and reliability of our platform. We do not sell personal data. Sharing is limited, controlled, and governed by strict contractual protections.

### 10.1 Categories of Recipients

Auko may share personal data with the following categories of recipients:

#### Cloud Infrastructure Providers

We use trusted cloud service providers to host and operate our platform. These providers supply compute, storage, networking, and security services essential to DrawCheck.

#### Authentication, Communication, and Support Tools

Certain providers support login, access management, email delivery, customer support platforms, and operational notifications.

### Monitoring, Security, and Logging Services

These providers process metadata only and never receive customer-uploaded drawings or standards.

### Professional Advisers

Accountants, auditors, legal advisers, and consultants may access limited personal data where necessary for their services.

### Payment and Billing Providers

These providers process billing contact information and payment metadata. Auko does not store full payment card details.

### Enterprise Customer Administrators

For business accounts, customer administrators may access information relating to their organisation’s users, account usage, and configuration.

### Law Enforcement and Regulatory Authorities

Personal data may be disclosed where required by law or to comply with valid legal processes.

Auko ensures that all recipients have appropriate privacy and security controls in place.

## 10.2 Subprocessors

Where Auko engages third-party service providers to process personal data on our behalf, those providers act as subprocessors. Auko:

- Conducts appropriate due diligence before onboarding suppliers
- Requires subprocessors to implement strong security and privacy safeguards
- Includes contractual obligations consistent with UK GDPR requirements
- Monitors subprocessors for continued compliance
- Provides information about subprocessors to customers on request

Subprocessors never use personal data for their own purposes.

## 10.3 Sharing of DrawCheck Content

DrawCheck Content (customer-uploaded drawings, standards, and related documents):

- Is processed only by Auko and approved infrastructure providers
- Is not shared with unrelated third parties
- Is not used for training or improving AI models
- Remains within the customer’s selected region (UK/EU or US)
- Is not visible to any entity other than Auko and the required cloud service provider
- Is deleted immediately after processing, except for customer standards retained for account operation

Auko does not outsource analysis of customer files to any external party and does not allow external reviewing of customer IP.

## 10.4 Sharing for Security and Fraud Prevention

Auko may share limited metadata with security service providers to:

- Detect or prevent security incidents
- Investigate unauthorised access attempts
- Monitor system integrity
- Comply with legal or regulatory obligations

These providers do not receive customer content or personal data beyond what is necessary for security purposes.

## 10.5 Corporate or Business Transactions

If Auko undergoes a merger, acquisition, or corporate restructuring, personal data may be shared with prospective or actual acquiring entities under strict confidentiality requirements. Any such transfer will respect applicable legal protections, and affected individuals will be informed where required.

## 10.6 No Sale of Personal Data

Auko does not:

- Sell personal data
- Rent personal data
- Allow third parties to use personal data for advertising or profiling
- Monetise customer data in any form

Personal data is used exclusively for the purposes described in this Notice.

## 10.7 Customer-Directed Sharing

Where a customer instructs Auko to integrate DrawCheck with other systems, Auko may transmit data according to those instructions. Auko does not share data with third-party integrations unless explicitly configured and approved by the customer.

### 10.8 International Considerations

Where sharing involves transfers outside the UK or EEA, Auko ensures appropriate safeguards are in place.

## 11. International Data Transfers

Auko Ltd primarily processes personal data within the United Kingdom and the European Economic Area (EEA). In certain circumstances, personal data may be transferred outside these regions. All such transfers occur in accordance with the UK GDPR and the Data Protection Act 2018.

Auko ensures that international transfers are lawful, limited, and protected by appropriate safeguards.

### 11.1 Primary Hosting and Processing Regions

Auko operates its platform in the following core regions:

- UK/EU region (default and primary hosting location)
- Optional US region (available upon explicit customer configuration)

Customers choosing the US region understand that personal data associated with their account may be processed in the United States.

Customer files (DrawCheck Content) remain strictly within the region selected by the customer.

### 11.2 Transfers to Third Countries

Where personal data is transferred outside the UK or EEA, Auko ensures that:

- The transfer is necessary and proportionate
- The recipient country provides an adequate level of protection or
- Appropriate safeguards are implemented under UK GDPR

Auko does not transfer personal data internationally unless such conditions are met.

### 11.3 Safeguards for International Transfers

Where required, Auko uses one or more of the following safeguards:

- Contractual protections aligned with UK GDPR requirements
- Supplier commitments and assurances regarding data protection
- Technical measures such as encryption, environment segregation, and access controls

- Regional processing restrictions enforced by the cloud provider

Auko does not rely on Privacy Shield or other frameworks deemed invalid by UK regulators.

## 11.4 Third-Party Providers Located Outside the UK/EU

Some subprocessors and supporting service providers may be based or operate outside the UK/EU. In these cases:

- Only the minimum necessary personal data is shared
- Providers must demonstrate compliance with applicable data protection standards
- Transfers are conducted using safeguards described above
- Providers may not use personal data for their own purposes

Customer-uploaded drawings and standards are never transferred to third countries beyond the region specifically chosen by the customer.

## 11.5 Customer-Directed International Transfers

If a customer integrates DrawCheck with external systems or configures processing in a non-UK/EU region:

- Auko processes data according to the customer’s explicit instructions
- The customer remains responsible for ensuring that its own transfers comply with applicable laws
- Auko acts as a Data Processor for such transfers

## 11.6 Limiting Unnecessary Transfers

Auko applies the principle of transfer minimisation:

- Processing is kept in-region whenever possible
- Metadata sent to external providers is limited and anonymised where feasible
- Customer content is never transmitted outside the selected region
- Internal access to data across regions is restricted

## 11.7 Transparency

Upon request, Auko provides:

- A list of relevant subprocessors
- The regions in which each service operates
- The safeguards used for transfer
- General information required for customer due diligence or international transfer assessments

# 12. Security Measures

Auko Ltd implements a comprehensive set of technical and organisational measures to protect personal data against unauthorised access, alteration, loss, or disclosure. These measures reflect the sensitivity of the data we handle, the nature of our services, and industry best practices, including guidance from the UK ICO and NCSC.

This section provides a high-level overview suitable for public transparency. More detailed internal controls are maintained separately.

## 12.1 Security Principles

Auko's approach to security is based on the following principles:

- **Confidentiality** – Personal data is only accessible to authorised individuals.
- **Integrity** – Systems and data are protected from unauthorised modification.
- **Availability** – Services and data are accessible when required.
- **Minimisation** – Personal data collection and retention are kept to the minimum necessary.
- **Segregation** – Environments and customer data are isolated.
- **Accountability** – Security responsibilities are clearly defined and documented.

## 12.2 Access Control

Auko enforces strict access control across all systems:

- Multi-factor authentication for all administrative access
- Role-based access control (RBAC) with the principle of least privilege
- Segregation of duties for operational and engineering roles
- Restricted production access (typically CTO-only, with controlled escalation)
- Authentication logs and monitoring to detect unusual behaviour
- Immediate revocation of access when no longer required

No employee or contractor has access to customer-uploaded drawings unless specifically authorised for operational reasons.

## 12.3 Encryption

All relevant data is encrypted:

- **In transit:** Using TLS 1.3 or equivalent secure protocols
- **At rest:** Using industry-standard cloud provider encryption mechanisms

Encryption keys are managed securely using cloud-native key management systems.

## 12.4 Network and Infrastructure Security

Auko operates a secure, cloud-native, serverless infrastructure designed to reduce attack surface:

- Segregated environments (development, staging, production)
- Separate cloud accounts to isolate environments and workloads
- No direct inbound access to compute services (all requests routed through secure API gateways)
- Web Application Firewall protection at ingress points
- DDoS protection through cloud provider services
- Hardened configuration baselines aligned with security best practice
- Automated deployment pipelines with version control, auditing, and change traceability

Infrastructure is monitored 24/7 using cloud-native security services.

## 12.5 Application and Data Security

Auko follows secure development and operational practices:

- Version-controlled code repositories
- Mandatory code review
- Automated scanning for vulnerabilities and misconfigurations
- Dependency monitoring and patch management
- Secure handling of credentials and secrets
- Testing that excludes customer content
- No logging of uploaded files or personal data contained within them
- Automatic deletion of customer drawings after processing

Customer standards and reports are stored with strict access controls.

## 12.6 Monitoring and Detection

Auko maintains monitoring systems to detect, prevent, and respond to threats:

- Automated alerting for suspicious activity
- Audit logging of security-relevant events
- Behavioural monitoring for abnormal patterns
- Regular review of authentication logs
- Guardrail mechanisms to prevent unauthorised access to customer data
- Security event escalation procedures

Logs contain metadata only and do not include customer drawings or personal content.

## 12.7 Supplier and Subprocessor Security

Auko ensures that its suppliers and subprocessors:

- Undergo risk assessment before onboarding
- Provide contractual assurances aligned with UK GDPR
- Maintain appropriate security certifications
- Implement strong security measures
- Are monitored periodically for continued compliance

Customer content is never processed by a subprocessor not approved for that purpose.

### 12.8 Organisational Security Measures

Auko complements technical security with organisational controls:

- Employee background screening appropriate to role
- Confidentiality agreements for all staff and contractors
- Mandatory security and data protection training
- Policies for acceptable use, data handling, remote work, and access control
- Defined incident response procedures
- Regular internal reviews of security posture

### 12.9 Incident Response

Auko maintains a documented incident response process that includes:

- Immediate investigation of suspected incidents
- Containment and mitigation steps
- Notification to affected customers
- Notification to the ICO when legally required
- Post-incident reviews and security improvements

Incidents involving DrawCheck Content are prioritised and handled under enhanced safeguards.

### 12.10 Continuous Improvement

Auko regularly evaluates and updates its security measures based on:

- New threats and vulnerabilities
- Regulatory requirements
- Changes to infrastructure or services
- Results from monitoring, audits, and assessments
- Industry best practice and NCSC/ICO guidance

## 13. Your Rights

Individuals whose personal data is processed by Auko Ltd have specific rights under the UK General Data Protection Regulation (UK GDPR). Auko is committed to respecting these rights and providing clear mechanisms for individuals to exercise them.

Where Auko acts as a **Data Controller**, individuals may exercise their rights directly with us. Where Auko acts as a **Data Processor** (primarily for DrawCheck Content), requests must be directed to the **customer organisation**, as they are the Data Controller.

## 13.1 Right of Access

Individuals have the right to request:

- Confirmation that Auko processes their personal data
- Access to that personal data
- A copy of the data in a commonly used format
- Information about how the data is used

Auko will respond within one month unless the request is unusually complex.

## 13.2 Right to Rectification

Individuals may request correction of inaccurate or incomplete personal data. Auko will update the data promptly or explain if correction cannot be made for legal or technical reasons.

## 13.3 Right to Erasure

Individuals may request that Auko delete personal data where:

- The data is no longer needed for its original purpose
- Consent (where used) is withdrawn
- Processing is unlawful
- There is no overriding legitimate interest for continued processing

This right may be limited where retention is required by law or necessary to establish or defend legal claims.

This right **does not apply** to DrawCheck Content processed on behalf of a customer; such requests must be made to the customer as Data Controller.

## 13.4 Right to Restrict Processing

Individuals may request that processing be restricted where:

- Accuracy of the data is contested
- Processing is unlawful
- A legal claim is pending

- A request to object is under review

Restricted data may still be stored but not otherwise used.

### 13.5 Right to Object

Individuals may object to the processing of personal data where the lawful basis is **legitimate interests**, unless Auko demonstrates compelling legitimate grounds to continue.

Individuals may also object at any time to **direct marketing**, and Auko will immediately cease such communications.

### 13.6 Right to Data Portability

Where processing is based on **contract** or **consent** and carried out by automated means, individuals may request their personal data:

- In a structured, commonly used, machine-readable format
- To be transferred directly to another controller where technically feasible

This right does not apply to DrawCheck Content, as Auko processes such data only on the customer's behalf.

### 13.7 Rights Relating to Automated Decision-Making

Auko does not perform automated decision-making that produces legal or significant effects on individuals. DrawCheck processes technical content, not personal data about individuals.

If this changes in the future, Auko will update this Notice accordingly.

### 13.8 Exercising Your Rights

To exercise any rights under UK GDPR, individuals may contact:
privacy@auko.ai

Auko may request identity verification before fulfilling certain requests to protect personal data.

### 13.9 Response Timeframes

Auko aims to respond to all valid requests:

- Within **one month**
- Within **two months** where requests are complex (with notification within the first month)

Requests that are manifestly unfounded or excessive may be refused or may incur a reasonable fee, as permitted by law.

### 13.10 Complaints

Individuals who believe their rights have not been respected may:

- Contact us directly to resolve the issue, or
- Lodge a complaint with the Information Commissioner’s Office (ICO), the UK data protection authority

ICO contact details are available at: https://www.ico.org.uk

## 14. Cookies and Tracking Technologies

Auko Ltd uses cookies and similar technologies on our website and web applications to ensure functionality, maintain security, and improve user experience. We do not use third-party advertising cookies, and we do not sell or share personal data for marketing purposes.

This section explains what technologies we use, why we use them, and how users can control their preferences.

### 14.1 What Are Cookies?

Cookies are small text files placed on a device when visiting a website. They allow websites to recognise devices and store certain information to support functionality and performance.

Cookies used by Auko do **not** provide access to a user’s device, files, or software.

### 14.2 Types of Cookies We Use

#### Essential Cookies

Required for the website and application to function. These cookies:

- Enable secure login and account management
- Maintain session integrity
- Support load balancing and service availability
- Ensure platform security

These cookies cannot be disabled without impairing core functionality.

#### Functional Cookies

Improve the user experience, such as:

- Remembering preferences (e.g., selected region or interface settings)
- Supporting in-browser application behaviour

These cookies do not track browsing outside the Auko environment.

#### Performance and Analytics Cookies

Used to understand how the website and application perform, including:

- Page load metrics
- Feature usage patterns
- Error rates and diagnostics

Analytics data is anonymised or pseudonymised wherever possible. Auko does **not** use advertising or cross-site tracking cookies.

### 14.3 Tracking Technologies We Do Not Use

Auko does **not** use:

- Behavioural advertising trackers
- Social media tracking pixels
- Third-party marketing cookies
- Fingerprinting technologies
- Cross-site tracking identifiers

We do not allow third parties to place advertising cookies on our website or application.

### 14.4 Use of Analytics Tools

Auko may use privacy-preserving analytics tools to understand aggregated usage trends. These tools process:

- Device and browser type
- Approximate geography (from IP)
- Session duration
- Feature usage
- Error messages and diagnostics

Analytics providers are not given access to customer drawings, standards, or any sensitive uploaded content.

### 14.5 Cookies Used in the DrawCheck Application

The DrawCheck web application may set cookies or local storage items that:

- Maintain login sessions

- Support authentication
- Store user interface preferences
- Ensure the security and integrity of processing workflows

No customer-uploaded files are stored in cookies, local storage, or browser caches.

### 14.6 How to Manage Cookies

Users may control or delete cookies at any time through:

- Browser settings
- Built-in privacy controls
- Cookie management tools provided by their browser

Blocking essential cookies will prevent the application from functioning properly.

### 14.7 Legal Basis for Cookies

The lawful basis depends on the type of cookie:

- **Essential cookies:** Legitimate interests (security, functionality)
- **Functional cookies:** Legitimate interests, or consent where required
- **Analytics cookies:** Legitimate interests or consent depending on tool configuration

Where consent is required, users will be provided with a clear choice.

### 14.8 Do Not Track (DNT)

The Auko website and application currently do not respond to browser-based Do Not Track signals. We continue to evaluate mechanisms that may support this preference in the future.

## 15. Children’s Data

Auko Ltd does not knowingly collect or process personal data relating to children. Our website, DrawCheck application, and associated services are designed for use by professionals in engineering, manufacturing, product development, and related fields. They are not directed toward children or individuals under the age of 18.

### 15.1 No Intended Use by Children

Auko’s services are strictly business-to-business (B2B). We do not offer products or services intended for children, and we do not target children in any form of communication or marketing.

### 15.2 Account Creation and Access Controls

To ensure that our services are used only by authorised adults:

- User accounts must be created by or under the authority of an employer or organisation
- Users must provide professional or company contact details
- We do not offer sign-up paths intended for or accessible to minors
- Age verification is not required because our services are not available to children in any context

## 15.3 No Processing of Children’s Personal Data

We do not:

- Collect personal data from children
- Process personal data about children
- Include children’s data in our workflows, logs, or AI analysis
- Intentionally accept files that contain information about minors

Any personal data about children that is accidentally included in customer-uploaded documents is treated as incidental data and immediately deleted when the underlying file is deleted.

## 15.4 If We Become Aware of Children’s Data

If Auko discovers that personal data relating to a child has been collected unintentionally:

- The data will be deleted as soon as reasonably possible
- We will inform the relevant customer organisation (as Data Controller) where appropriate
- We will take steps to prevent recurrence

## 15.5 Customer Responsibilities

Customers are responsible for ensuring that:

- They do not upload documents that contain information about minors
- DrawCheck is used only by authorised adult employees
- Any incidental inclusion of children’s data is avoided

Auko provides guidance to customers to minimise accidental inclusion of personal data of any kind.

# 16. Marketing Communications

Auko Ltd engages in limited business-to-business (B2B) marketing to keep customers and prospective customers informed about our products, updates, and services. We do not engage in consumer marketing, behavioural advertising, or the sale of personal data.

## 16.1 Types of Marketing Communications

Auko may send the following types of marketing messages:

- Product updates and new feature announcements
- Invitations to webinars, demonstrations, or events
- Industry insights and engineering-related content
- Information about new services or enhancements
- Company news relevant to customers and partners

We do not send high-frequency or unsolicited promotional material.

## 16.2 Lawful Basis for Marketing

Auko relies on one of the following lawful bases:

### Consent

Used where individuals explicitly opt in to receive marketing communications, such as:

- Subscribing via the website
- Opting in during account creation
- Requesting updates via email

Consent can be withdrawn at any time.

### Legitimate Interests

Used for low-impact B2B outreach to professionals where:

- They have shown interest in Auko’s services
- They represent an organisation that may reasonably expect contact
- The communication is relevant to their professional role
- A clear opt-out is provided in every message

This approach aligns with the UK ICO’s guidance on B2B marketing.

## 16.3 How to Manage Your Preferences

Individuals may opt out of marketing at any time by:

- Clicking the unsubscribe link in any marketing email
- Updating communication preferences (where available)
- Contacting Auko directly at: privacy@auko.ai

Preferences are respected immediately or as soon as reasonably possible.

### 16.4 Information Used for Marketing

Auko uses only the minimum necessary information for marketing, such as:

- Name
- Professional email address
- Company name
- Job role
- Marketing preferences (opt in/opt out)

We do not use customer-uploaded drawings, standards, or technical documents for marketing under any circumstances.

### 16.5 No Third-Party Advertising or Sales of Data

Auko does not:

- Share personal data with third parties for advertising
- Conduct retargeting or cross-site tracking
- Buy or sell marketing lists
- Permit advertising cookies on our website
- Use social media pixels
- Engage in automated profiling for marketing

Marketing is strictly professional and non-intrusive.

### 16.6 Service and Transactional Emails

Certain emails related to the operation of the DrawCheck service are **not** considered marketing, including:

- Account creation and activation messages
- Password reset emails
- Security alerts
- Notices about platform changes affecting service delivery
- Billing and subscription communications
- Scheduled maintenance notifications

These communications are necessary for providing the service and cannot be opted out of.

# 17. Data Sharing with Third Parties

Auko Ltd shares personal data with third parties only where necessary to operate our services, fulfil contractual or legal obligations, or ensure the security and reliability of our platform. All third parties are subject to strict contractual requirements, and data sharing is limited to the minimum necessary for the relevant purpose.

## 17.1 Categories of Third Parties We Work With

### Cloud Hosting and Infrastructure Providers

These providers supply compute, storage, networking, encryption, and regional hosting capabilities used by the DrawCheck platform. They may process:

- Account identifiers
- Application metadata
- User authentication events
- Temporary access tokens
- DrawCheck Content for processing (in-region only)

These providers do **not** use personal data or DrawCheck Content for their own purposes.

### Authentication, Access Management, and Communication Providers

These services support:

- Secure login
- Multi-factor authentication
- Email delivery
- Secure communication with users
- System notifications

They may process email addresses, IP addresses, and basic account metadata.

### Operational Monitoring and Error Tracking Providers

These providers receive:

- Metadata-only logs
- Error status codes
- System performance metrics

They do **not** receive uploaded drawings, standards, reports, AI outputs, or any sensitive content. Sensitive data is stripped or sanitised before transmission.

### Payment Processors and Billing Platforms

These services process:

- Company billing details
- Billing contact information
- Subscription activity
- Payment confirmation metadata

Auko does not store full card numbers or payment instruments.

#### Professional Advisers

Auko may share limited records with:

- Accountants
- Legal advisers
- Auditors
- Insurance-related assessors

These advisers act under confidentiality agreements and process only what is necessary for their role.

#### Third-Party Security and Compliance Providers

These providers assist with:

- Security monitoring
- Threat detection
- Vulnerability scanning
- Compliance verification

Only metadata necessary for security is shared.

### 17.2 Subprocessors Acting on Behalf of Auko

Where Auko engages third parties to process personal data on our behalf, they act as **subprocessors**. Auko ensures that subprocessors:

- Undergo security and privacy due diligence
- Implement appropriate technical and organisational measures
- Sign contractual agreements meeting UK GDPR standards
- Are subject to ongoing review and monitoring
- Process personal data only under Auko’s documented instructions

A list of subprocessors is available to customers on request and is maintained as part of our customer-facing documentation.

### 17.3 DrawCheck Content: Strictly Controlled Sharing

DrawCheck Content—including drawings, standards, and any uploaded files—is subject to the highest level of protection:

- Shared **only** with cloud infrastructure and AI provider components required to process the file
- Processed **solely** within the customer-selected region (UK/EU or optional US region)
- Never shared with unrelated third parties
- Never used by providers to train AI models
- Never transmitted to analytics, monitoring, or error-tracking systems
- Deleted immediately after processing (with limited 24-hour retention after failures)

Auko does not use third-party contractors or external reviewers to handle customer IP.

## 17.4 Customer-Directed Integrations

Where customers request integrations with external systems:

- Auko will transmit only the data needed for the integration. Customers act as the Data Controller for such transfers
- Auko is not responsible for the third party's compliance or security
- Customers may disable integrations at any time

No integrations are enabled by default, and none involve sharing DrawCheck Content without explicit direction.

## 17.5 Legal and Regulatory Requirements

Auko may disclose personal data where required to:

- Comply with applicable law
- Respond to valid law enforcement requests
- Meet regulatory or judicial obligations

Auko:

- Carefully evaluates each request
- Minimises the data disclosed
- Notifies the customer where legally permitted

Auko does not provide direct access to systems or datasets to government authorities.

## 17.6 Business Transfers

If Auko is involved in a merger, acquisition, investment, restructuring, or sale of assets:

- Personal data may be disclosed under confidentiality agreements
- Only the minimum necessary data is shared for due diligence

- Affected parties will be informed where required by law
- Any successor entity will be bound by terms consistent with this Privacy Notice

### 17.7 What We Do Not Share

Auko does **not** share:

- Customer drawings or standards with any entity other than required infrastructure providers
- Personal data for advertising or marketing by third parties
- Personal data with data brokers
- Information with social media or advertising networks
- AI outputs outside the customer environment
- Logs containing sensitive or customer content

Our data sharing is purpose-driven, tightly controlled, and transparently governed.

## 18. Data Security

Auko Ltd is committed to protecting personal data and customer intellectual property using security measures aligned with industry best practices, UK GDPR requirements, and guidance from the UK National Cyber Security Centre (NCSC) and the Information Commissioner’s Office (ICO). Security is embedded throughout our infrastructure, development processes, and operational practices.

### 18.1 Security Approach

Auko’s security programme is built on core principles:

- Ensuring confidentiality, integrity, and availability of systems and data
- Implementing proportional and risk-based safeguards
- Minimising the collection and retention of personal data
- Segmenting and isolating environments and customer data
- Maintaining accountability through documented policies and procedures

Security is considered at every stage of system design and operation.

### 18.2 Technical Measures

#### Encryption

All relevant personal data is encrypted:

- In transit using TLS 1.3 or equivalent
- At rest using cloud-provider-managed encryption keys

### Access Control

Auko enforces:

- Multi-factor authentication
- Role-based access control
- Principle of least privilege
- Strict limitation of production access (typically CTO-only)
- Monitoring of access events

### Network and Infrastructure Security

Auko uses:

- Segregated cloud accounts for development, staging, and production
- Serverless architecture with no publicly exposed compute nodes
- Secure API gateways
- Web Application Firewall protection
- Automated patching and vulnerability detection
- DDoS mitigation and protective services

### Application Security

We employ:

- Secure coding practices
- Code reviews for all changes
- Automated dependency and vulnerability scanning
- Secrets management using secure cloud-native services
- Strict prohibition on logging customer content
- Automated deletion of uploaded files

## 18.3 Organisational Measures

Auko maintains:

- Confidentiality agreements for all staff and contractors
- Background screening appropriate to role
- Mandatory data protection and security training
- Defined onboarding and offboarding procedures
- Policies for acceptable use, remote work, and data handling

Auko employees and contractors are permitted access only where necessary for their role.

## 18.4 Supplier Security

Before engaging a supplier or subprocessor, Auko conducts:

- Security and privacy due diligence
- Assessment of certification (e.g., ISO 27001, SOC 2) where relevant
- Review of technical and organisational measures
- Contractual checks to ensure UK GDPR-aligned obligations

Suppliers are monitored periodically for continued compliance.

### 18.5 Incident Detection and Response

Auko maintains processes for:

- Continuous monitoring of system activity
- Automated alerting on anomalous behaviour
- Investigating potential security incidents
- Containing and remediating confirmed incidents
- Notifying affected customers promptly
- Reporting to the ICO where legally required

Incidents involving customer IP or personal data are prioritised.

### 18.6 Customer Responsibilities

Customers also play a role in maintaining security by:

- Managing user access and permissions within their organisation
- Protecting credentials and MFA devices
- Avoiding the upload of unnecessary personal or sensitive data
- Following guidance provided through Auko’s documentation

Customer administrators remain responsible for internal user management.

### 18.7 Continuous Improvement

Auko continually reviews and enhances its security controls based on:

- Threat and vulnerability intelligence
- Platform changes
- Supplier updates
- Regulatory developments
- Feedback from customers
- Findings from internal assessments and testing

Security is not a one-time effort; it is an ongoing commitment.

## 19. Changes to This Privacy Notice

Auko Ltd may update this Privacy Notice from time to time to reflect changes in our services, legal requirements, or how we process personal data. We are committed to maintaining transparency and ensuring individuals remain informed about how their data is used.

### 19.1 When We Make Changes

Updates may occur when:

- We introduce new features or services
- Our data processing activities change
- Our suppliers or subprocessors change
- Legal or regulatory requirements evolve
- Security or operational practices are updated

Changes are made only where necessary and are reviewed internally before publication.

### 19.2 How We Communicate Changes

When the Privacy Notice is updated:

- The latest version will always be published on our website
- A revised **“Last Updated”** date will be displayed at the top
- For material changes affecting individuals, we will provide additional notice, which may include email communication or in-app notification

Changes that significantly affect how personal data is processed will be highlighted clearly.

### 19.3 Version Control

Each update is recorded using a structured version numbering format (e.g., *v1.0, v1.1, v2.0*) to make it easy to identify revisions.
Archived versions may be made available on request where required for audit or procurement processes.

### 19.4 Ongoing Updates

Auko reviews this Privacy Notice periodically to ensure it remains accurate and compliant. By continuing to use our website or services after changes are published, individuals acknowledge the updated Notice, unless additional consent is required by law.

## 20. Contact Details

If you have any questions about this Privacy Notice, how your personal data is processed, or if you wish to exercise your rights under the UK GDPR, you can contact Auko Ltd using the details below.

## 20.1 Contacting Auko Ltd

**Email:**
guy@auko.ai

**Address:**
Auko Ltd
51 Church Lane
Sevenhampton, Cheltenham
GL54 5SW, UK

## 20.2 Data Protection Queries

For questions related specifically to data protection, legal compliance, or individual rights, please contact the email address above. These queries are handled by the CTO, with oversight from the CEO.

## 20.3 Complaints to the ICO

If you are dissatisfied with how Auko handles your personal data, you may lodge a complaint with the UK's supervisory authority:

**Information Commissioner's Office (ICO)**
Website: https://www.ico.org.uk
Telephone: +44 (0)303 123 1113

Auko encourages individuals to contact us first so we can work to resolve any concerns.

## 20.4 Exercising Your Rights

All requests under Sections 13 (Your Rights) should be sent to:
rich@auko.ai

Auko may request proof of identity to ensure personal data is not disclosed improperly.

## Version history

| | |
|---|---|
| **Version** | 1.2 |
| **Date** | 15/02/2025 |
| **Author** | Richard Comber |
| **Reviewed by** | Guy Cowdry |