# PRIVACY POLICY

*Aurex™ Website and GRC Platform*

*Public Notice*

| | |
|---|---|
| **Document ID** | PPY-AUREX-PUBLIC-2026-001 |
| **Version** | 1.0 |
| **Effective Date** | 29 September 2026 |
| **Applies To** | Visitors to aurex.ai and users of the Aurex GRC platform |
| **Data Controller** | Aurex™ |
| **Contact** | privacy@aurex.ai |
| **Classification** | Public |

## 1. Introduction

This Privacy Policy explains how Aurex™ ("Aurex", "we", "us") collects, uses, discloses and protects personal data when you visit our website or use the Aurex Governance, Risk and Compliance (GRC) platform ("Aurex GRC").

Aurex works with Beinex, a subservice provider, for certain engineering, quality assurance, DevOps and security operations functions. This Policy applies equally to personal data processed by Beinex on Aurex's behalf.

## 2. Who This Policy Covers

This Policy applies to personal data collected through our website, the Aurex GRC platform, and in the course of our business relationship with clients and their users.

- Where you are a visitor to our website or contact us directly (for example, sales or support enquiries), Aurex is the Data Controller.
- Where your organization ("the client") uses the Aurex GRC platform, the client is the Data Controller for the content it uploads and Aurex acts as Data Processor on the client's instructions.

## 3. Information We Collect

| Category | Examples |
|---|---|
| **Account Information** | Name, work email address, employee ID, job title and department – used for authentication, system access and role assignment |
| **Platform Content** | Risk assessments, audit findings, incident reports and similar business content supplied by your organization |
| **Communication Data** | Messages, comments and feedback submitted within the application |
| **Technical Data** | IP address, browser type, device and operating system information |

| Category | Examples |
|---|---|
| **Usage Data** | Login times, pages visited, features used |
| **Website Data** | Cookies and similar technologies – see Section 9 |

## 4. Legal Basis for Processing

| Processing Activity | Legal Basis |
|---|---|
| **User account management** | Performance of contract |
| **GRC process execution (risk, audit, compliance workflows)** | Legitimate interests of the client organization |
| **System analytics and performance monitoring** | Legitimate interests (service improvement) |
| **Compliance and regulatory reporting** | Legal obligation |
| **Non-essential cookies and optional processing** | Consent (withdrawable at any time) |
| **Security monitoring and incident response** | Legitimate interests (protecting system and data integrity) |

## 5. How We Use Your Information

We use personal data to provide and maintain the Aurex GRC platform, authenticate users, deliver the features your organization has configured, respond to support requests, monitor and improve security and performance, and meet our legal and contractual obligations. We do not sell personal data.

## 6. Data Retention

We retain personal data only for as long as necessary for the purposes described in this Policy, or as required by law or contract. Account information is generally retained for the duration of the user's account plus a limited period after deactivation; platform content is retained in line with your organization's contract with us; technical and usage data is retained for shorter periods tied to security and analytics needs.

## 7. Data Sharing and Disclosure

We share personal data only where necessary to deliver the service, and always under a written data processing agreement:

- Cloud hosting and infrastructure providers, for hosting and storage.
- Email and communication providers, for system notifications and support.
- Application performance monitoring providers, for system health and troubleshooting.
- Identity and authentication providers, for secure sign-in.

We do not share personal data with third parties for their own marketing purposes. A current list of sub-processors is available on request to security@beinex.com.

## 8. Data Security

We maintain a range of technical and organizational measures to protect personal data, including:

- Encryption of data in transit and at rest.
- Role-based access controls and multi-factor authentication.
- Regular security testing, including vulnerability scanning and penetration testing.
- Continuous monitoring and logging of access to production systems.

## 9. Cookies and Tracking Technologies

Our website uses essential cookies to operate securely and, with your consent, non-essential cookies for analytics and to remember your preferences. When you first visit aurex.ai, a cookie banner lets you accept, reject, or choose which optional categories to allow; you can change your choice at any time through the cookie preferences link in the site footer. Essential cookies do not require consent.

## 10. International Data Transfers

Personal data may be transferred to and processed in countries other than your own. Where this occurs, we rely on an appropriate transfer mechanism, such as an adequacy decision, Standard Contractual Clauses, or your organization's own approved intra-group transfer mechanism, together with appropriate technical and organizational safeguards.

## 11. Your Privacy Rights

| Right | How to Exercise It |
|---|---|
| **Access** | Request confirmation of whether we process your data and obtain a copy – privacy@aurex.ai |
| **Rectification** | Correct inaccurate or incomplete data – via your user profile or privacy@aurex.ai |
| **Erasure** | Request deletion where there is no compelling reason for continued processing – privacy@aurex.ai |
| **Restriction** | Limit how your data is used while a request is resolved – privacy@aurex.ai |
| **Portability** | Receive your data in a structured, machine-readable format – privacy@aurex.ai |
| **Object / Withdraw Consent** | Object to processing or withdraw consent at any time, with no effect on access to the service – privacy@aurex.ai |
| **Complain** | Lodge a complaint with your local data protection authority |

Where Aurex acts as Data Processor for content your organization has uploaded, we forward requests we receive directly to your organization, which is responsible for responding as Data Controller.

## 12. Consent, Choice and Withdrawal

Where processing is based on consent, such as non-essential cookies or marketing communications, the following principles apply:

- Consent is never bundled with acceptance of our terms of use or any other consent.
- Withdrawing consent is no more difficult than giving it and has no effect on your access to the service.
- Refusing optional processing never affects the functionality, support, or pricing available to you.

## 13. Special Categories of Personal Data

The Aurex GRC platform is not designed to collect special category data (such as health, biometric, racial or ethnic origin, religious belief, or trade union membership) and does not require it for normal use. Where a client determines that such data is necessary for its own audit or compliance scenarios, processing occurs only with an appropriate legal basis and additional safeguards, including optional column-level data masking.

## 14. Automated Decision-Making and Profiling

Aurex does not use personal data to make decisions that produce legal or similarly significant effects about individuals through fully automated means, without human involvement.

## 15. Breach Notification

If a personal data breach occurs that is likely to affect you, we will notify affected clients without undue delay and in accordance with applicable law, and will support notification to individuals and regulators where required.

## 16. Changes to This Policy

We may update this Policy from time to time to reflect changes in our practices or in applicable law. The “Effective Date” at the top of this Policy shows when it was last revised. Material changes will be notified to clients and users through the application or by email.

## 17. Contact Us

For any question about this Policy or to exercise your privacy rights, contact us at privacy@aurex.ai, or write to our security team at security@beinex.com.