



# Privacy Policy

**Total-Applications Platform & Advisory Services**

Last Updated: February 2026

---

## 1. Introduction

This Privacy Policy explains how personal data is collected, used, stored, and protected in connection with:

- The sale and licensing of digital products, frameworks, documents, and architectural materials
- Access to platform-based tools, including AI/GPT companions and advisory assistants
- Project architecture advisory and consulting services
- Technical support and implementation guidance
- Website access and related communications
- All other services, tools, or materials provided by Total-Applications Ltd

This policy applies to all users of the platform, including:

- Visitors
- Licence holders
- Advisory clients
- GPT or AI tool users
- Support clients
- Authorised organisational users

This platform may be used for various project types, including (but not limited to):

- AEM architecture
- Headless implementations
- Front-end design
- Digital transformation
- AI agent design
- Enterprise systems
- General software architecture

We are committed to handling personal data responsibly and in accordance with applicable data protection laws, including UK GDPR and EU GDPR where applicable.

## 2. Data Controller

The data controller responsible for personal data described in this policy is:

Christopher Williams  
Total-Applications Ltd  
Plum Tree Farm  
Doncaster  
DN14 9AG  
United Kingdom  
Email: [chris@total-applications.com](mailto:chris@total-applications.com)

---

## 3. What Personal Data We Collect

We collect only the data necessary to operate and support the platform and related services.

### 3.1 Purchase and Licence Data

When you purchase or license any product or service, we may collect:

- Full name
- Organisation name
- Job title (if provided)
- Email address
- Billing address
- VAT number (if applicable)
- Purchase history
- Licence tier
- Payment status

We do not store full payment card details. Payments are processed by secure third-party payment providers.

---

### 3.2 Platform & AI Tool Access Data

If you access the platform, documents, GPT companions, AI assistants, or other advisory tools, we may collect:

- Authorised user name
- Organisation affiliation
- Email address
- Access logs (date/time of access)
- High-level usage metrics (e.g., frequency of use, feature usage categories)

We do not intentionally collect or store full AI conversation content unless required for:

- Service integrity
- Abuse detection
- Security monitoring

- Compliance or dispute resolution
- Improving system behaviour in a controlled and secure manner

Users are responsible for ensuring they do not submit sensitive or regulated personal data unless covered by a separate written agreement.

---

### **3.3 Advisory and Support Services Data**

If you engage in consulting, advisory sessions, retainers, or technical support, we may process:

- Contact information
- Organisation details
- Meeting details
- Project-related information shared during discussions
- Notes or documentation created as part of the engagement

Where confidential information is shared under NDA, it is handled in accordance with that agreement.

---

### **3.4 Website and Technical Data**

When you visit our website or platform, we may collect:

- IP address
- Browser type
- Device type
- Basic analytics data (e.g., page visits, referral source)
- Security logs

This data is used solely for:

- Security
  - Fraud prevention
  - Platform stability
  - Performance monitoring
- 

## **4. Lawful Basis for Processing**

We process personal data under the following lawful bases:

### **Contractual Necessity**

To:

- Provide licensed materials
- Grant access to platform tools
- Deliver advisory or support services
- Manage accounts
- Process payments

## Legitimate Interests

To:

- Protect intellectual property
- Prevent licence misuse
- Maintain platform security
- Improve service quality
- Manage business operations

## Legal Obligations

To:

- Comply with tax and accounting regulations
- Maintain financial records
- Respond to lawful regulatory requests

## Consent (Where Applicable)

For:

- Optional marketing communications
- Non-essential cookies

You may withdraw consent at any time.

---

## 5. How We Use Personal Data

We use personal data only for:

- Processing purchases and licences
- Providing access to digital materials and platform tools
- Delivering AI and GPT-based advisory assistance
- Delivering consulting and support services
- Communicating important service updates
- Maintaining platform security
- Preventing misuse or abuse
- Complying with legal requirements

We do not sell personal data.

---

## 6. AI and GPT-Based Services

Where AI services are provided:

- User queries may be processed via third-party AI service providers.
- We configure services, where possible, to disable training on submitted content.
- We do not intentionally use your data to train public AI models.

- Usage data may be logged for security and compliance monitoring.

Users should not submit:

- Sensitive personal data
- Health information
- Financial account numbers
- Government ID numbers
- Classified or regulated information

Unless covered by a separate written agreement.

---

## 7. Payment Processing

Payments are handled by secure third-party payment providers (e.g., Stripe or similar platforms).

We do not store:

- Full card numbers
- CVV codes
- Banking login credentials

Payment providers operate under their own privacy policies.

---

## 8. Data Retention

We retain personal data only for as long as necessary.

Typical retention periods:

- Licence and billing records: 6–7 years (tax compliance)
- Platform access logs: reasonable operational period
- Advisory records: as defined in engagement terms
- Website analytics data: limited operational period

When data is no longer required, it is securely deleted or anonymised.

---

## 9. Data Security

We implement appropriate technical and organisational measures, including:

- Secure hosting environments
- Encrypted connections (HTTPS)
- Role-based access controls
- Limited internal access
- Monitoring for unauthorised activity

However, no system can guarantee absolute security.

---

## 10. International Transfers

Where infrastructure providers or AI providers operate outside the UK or EU:

- Transfers are made with appropriate safeguards
  - Standard contractual clauses may apply
  - Providers are selected based on security and compliance posture
- 

## 11. Your Rights

Under applicable data protection law, you may have the right to:

- Access your personal data
- Request correction
- Request deletion (subject to legal obligations)
- Restrict processing
- Object to processing
- Request data portability (where applicable)
- Withdraw consent

To exercise these rights, contact us at:

[chris@total-applications.com](mailto:chris@total-applications.com)

---

## 12. Confidentiality and NDAs

Where services are delivered under NDA:

- Confidential information is handled separately
  - It is not used beyond the agreed purpose
  - Additional contractual safeguards may apply
- 

## 13. Children's Data

Services are not directed at individuals under 18. We do not knowingly collect data from children.

---

## 14. Changes to This Policy

We may update this Privacy Policy from time to time.

The "Last Updated" date will reflect revisions.

Continued use of the platform or services constitutes acceptance of the updated policy.

---

## 15. Contact Information

For privacy-related enquiries:

chris@total-applications.com

Total-Applications Ltd

If you are located in the UK, you may also contact the Information Commissioner's Office (ICO) if you believe your data has been handled improperly.

---

## Important Strategic Advice

Right now your business is expanding beyond AEM.

Your legal documentation must reflect **platform capability, not one product niche**.

If you don't generalise now, you'll constantly be rewriting legal docs every time you add:

- A new GPT
- A new framework
- A new industry
- A new advisory offer

This version protects you long-term.

If you'd like, I can now:

- Tighten this further into a more enterprise-polished tone
- Align it with your Terms & Conditions
- Or produce a separate AI Data Processing Addendum (which larger clients may eventually ask for)