DATA PROCESSING AGREEMENT - DOMANENNAME

Processor Data Protection Obligations

Version: 1.0 Effective Date: 18th May 2026 Company: CRISALEO LIMITED Operating Domains: domanenname.com | domanenname.it | domanenname.eu | domanenname.us | domanenname.de

Governing Law: The laws of England and Wales \(English Law\), with GDPR compliance for applicable territories Jurisdiction: Courts of England and Wales

---

1. INTRODUCTION

This Data Processing Agreement \("DPA"\) establishes the terms under which CRISALEO LIMITED \("the Processor"\) processes personal data on behalf of customers \("the Controllers"\) in accordance with:

- UK General Data Protection Regulation \(UK GDPR\) - Data Protection Act 2018
- EU General Data Protection Regulation \(GDPR\) - EU Regulation 2016/679
- CCPA \(California Privacy Rights Act\) - for California residents
- Local data protection laws - applicable jurisdictions

This DPA is an essential addendum to Domanenname’s Terms of Service and Privacy Policy.

---

2. DEFINITIONS

2.1 Key Terms

- Personal Data: Any information relating to an identified or identifiable natural person
- Processing: Any operation performed on personal data \(collection,) Tj ET BT /

- Controller: Customer who determines the purpose and means of processing \(Domanenname customer\)
- Processor: CRISALEO LIMITED / Domanenname - provides processing services
- Sub-Processor: Any third party engaged by the Processor to process data
- Data Subject: Individual to whom personal data relates

- Recipient: Any person or entity receiving personal data
- Data Breach: Unauthorized or accidental disclosure of personal data
- GDPR: General Data Protection Regulation \(EU/UK legislation\)
- Consent: Clear, freely given permission to process data
- Legitimate Interest: Processor’s valid reason to process data
- Special Category Data: Sensitive data requiring heightened protection

2.2 Roles

Domanenname Role: PROCESSOR

- Domanenname is a Data Processor, not a Data Controller
- Domanenname processes data on customer’s instructions
- Domanenname is not the legal entity responsible for processing decisions

Customer Role: CONTROLLER

- Customer is the Data Controller
- Customer determines what data is collected and why
- Customer is primarily responsible for GDPR compliance

---

3. SCOPE OF PROCESSING

3.1 Personal Data Processed

Domanenname processes the following personal data on behalf of customers:

3.1.1 Domain Registrant Data \(ICANN-Required\)

- Full name and surname
- Postal address \(complete\)
- Email address
- Telephone number
- Company/Organisation name \(if applicable\)
- Country/jurisdiction

Legal Basis for Processing: ICANN mandatory requirements; contract performance

Retention: Duration of domain registration + 1 year post-cancellation \(ICANN audit requirement\)

3.1.2 Administrative and Technical Contacts

- Contact name and email

- Telephone number
- Organisation

Legal Basis: Contract performance and domain technical management

Retention: Duration of domain registration + 6 months

3.1.3 Billing and Payment Data

- Cardholder name
- Billing address
- Last 4 digits of payment card
- Payment method used
- Transaction history
- Invoice records

Legal Basis: Contract performance; legal obligation \(tax records\)

Retention: Full payment history retained for 10 years \(UK tax) Tj ET BT /F1 11

Note: Full credit card numbers are NOT processed or stored by Domanenname

3.1.4 Access and Account Data

- Username/email used for login
- IP addresses used for access
- Login timestamps
- Device information
- Browser information
- Session data

Legal Basis: Legitimate interest \(security\); contract performance

Retention: 12 months for security logs; 24 hours for active sessions

3.1.5 Communication Data

- Support emails and chat transcripts
- Correspondence with customer
- Feedback and complaints
- Newsletter subscriptions \(if opted in\)

Legal Basis: Contract performance; legitimate interest; consent

Retention: 24 months \(dispute resolution\); 12 months standard

3.2 Purposes of Processing

Domanenname processes personal data for:

| Purpose | Legal Basis | Retention |
|---|---|---| | Domain registration and management | Contract | Registration duration | | Billing and payment | Legal obligation | 10 years \(tax\) | | Customer support | Contract | 24 months | | Service communication | Contract + Legitimate interest | Duration | | Security and fraud prevention | Legitimate interest | 12 months | | System maintenance and backups | Legitimate interest | Backup duration | | Law enforcement compliance | Legal obligation | As required by law | | ICANN audit compliance | Legal obligation | 12 months post-cancellation | | Service improvements | Legitimate interest | Until anonymised |

3.3 Categories of Data Subjects

Personal data is collected from/about:

- Individual domain registrants
- Administrative contacts for domains
- Technical contacts for domains
- Billing contacts and account holders
- Support request submitters
- Email recipients \(for communications\)
- Website visitors \(limited technical data\)

---

4. PROCESSOR OBLIGATIONS

4.1 Core Processing Requirements

Domanenname \(as Data Processor\) commits to:

4.1.1 Processing on Instructions Only

- Personal data processed only on documented customer instructions
- Data not processed for Domanenname’s own purposes \(except as) Tj ET BT /F1 1

- If customer instructions conflict with law, Domanenname will notify customer
- New purposes require customer written approval

4.1.2 Confidentiality

- All staff accessing personal data bound by confidentiality obligations
- Staff members trained on data protection and confidentiality
- Confidentiality obligations survive employment termination
- Third parties subject to written confidentiality agreements

4.1.3 Data Security

- Implement technical and organisational security measures \(Section) Tj ET BT /

- Protect personal data against unauthorised or unlawful processing
- Protect against accidental loss, destruction, or damage
- Regularly test security measures
- Maintain incident response procedures

4.1.4 Compliance with GDPR Articles

Domanenname complies with applicable GDPR articles including:

- Article 32: Security of processing
- Article 33: Breach notification
- Article 34: Communication with data subjects
- Article 35: Data Protection Impact Assessment
- Article 36: Prior consultation with supervisory authority
- Article 37: Appointment of Data Protection Officer

4.2 Subject Rights Support

Domanenname provides reasonable assistance to customers for:

4.2.1 Right of Access \(Article 15\)

- Customer requests personal data held about a data subject
- Domanenname extracts and provides data in common format
- Supports customer in responding to data subject access requests

4.2.2 Right to Rectification \(Article 16\)

- Data subject requests correction of inaccurate data
- Domanenname implements corrections requested by customer
- Confirms correction to data subject

4.2.3 Right to Erasure \(Article 17\)

- Data subject requests deletion
- Domanenname deletes data \(subject to legal retention requirements\)
- Confirms deletion to data subject
- Notifies Sub-Processors of deletion

4.2.4 Right to Restrict Processing \(Article 18\)

- Customer requests processing restriction
- Domanenname restricts processing of flagged data
- Maintains data but does not process except with customer authorisation

4.2.5 Right to Data Portability \(Article 20\)

- Customer requests data in machine-readable format
- Domanenname provides in CSV, JSON, or XML format
- Supports transfer to another processor if requested

4.2.6 Right to Object \(Article 21\)

- Data subject objects to processing
- Customer notified of objection
- Domanenname suspends processing pending customer instruction

4.2.7 Rights Regarding Automated Decision-Making \(Article 22\)

- Domanenname does not use fully automated decision-making with legal effect
- Domain suspension/cancellation involves human review
- Data subject has right to human review

4.3 Transparency and Documentation

Domanenname maintains:

- Records of Processing Activities: Detailed documentation of all processing
- Privacy Notices: Clear explanations of data use
- This DPA: Formal agreement establishing processor role
- Privacy Policy: Available to all customers
- Audit Trails: Records of who accessed data and when

---

5. DATA SECURITY MEASURES

5.1 Technical Security Controls

5.1.1 Encryption

- In Transit \(TLS/SSL\): All data transmitted via HTTPS with TLS 1.2 or higher
- At Rest: Database encryption using AES-256 or equivalent
- Backup: Encrypted backups stored separately
- Key Management: Encryption keys managed securely, not stored with encrypted data

5.1.2 Access Controls

- Authentication: Unique usernames and strong passwords required
- Multi-Factor Authentication \(MFA\): 2FA available; recommended for staff

- Role-Based Access Control \(RBAC\): Staff access limited to necessary data
- Principle of Least Privilege: Minimal access grants by default
- Segregation of Duties: Critical functions require multiple staff members

5.1.3 Infrastructure Security

- Firewall: Perimeter firewall with intrusion detection/prevention
- Web Application Firewall \(WAF\): Cloudflare WAF protecting against attacks
- DDoS Protection: Cloudflare DDoS mitigation
- Intrusion Detection: 24/7 network monitoring
- Secure Baselines: Servers hardened per security benchmarks

5.1.4 Monitoring and Detection

- Anomaly Detection: AI-powered monitoring for unusual activity
- Log Monitoring: Real-time alerts for suspicious events
- File Integrity Monitoring: Detection of unauthorised file changes
- Vulnerability Scanning: Weekly automated scans
- Penetration Testing: Annual third-party testing

5.2 Organisational Security Measures

5.2.1 Personnel Security

- Background Checks: Conducted before employment
- Security Training: Annual mandatory training on data protection
- Confidentiality Agreements: All staff sign binding agreements
- Need-to-Know: Staff access data only if necessary for role
- Termination Process: Access revoked upon employment termination

5.2.2 Physical Security

- Data Centre Security: Facilities managed by certified providers
- Access Controls: Badge access and biometric controls
- CCTV: Video surveillance of data centre areas
- Environmental Controls: Fire suppression and temperature control
- Backup Location: Geographically separate from primary

5.2.3 Governance and Compliance

- Data Protection Officer: Appointed DPO overseeing compliance
- Data Protection Impact Assessment: Conducted for high-risk processing
- Data Processing Records: Maintained per GDPR requirements

- Incident Response Plan: Documented procedures for breaches
- Annual Audit: Third-party security audits conducted

5.3 Certifications and Standards

Domanenname complies with:

- ISO 27001: Information security management system
- PCI-DSS Level 1: Payment card data security
- SOC 2 Type II: Service organisation controls
- GDPR Article 32 Requirements: Security obligations
- UK Data Protection Act 2018: UK law compliance

---

6. SUB-PROCESSORS AND INTERNATIONAL TRANSFERS

6.1 Sub-Processors

Domanenname engages sub-processors to:

- Registry Partners: Process domain registration data
- Payment Processors: Process billing data
- Cloud Infrastructure: Host systems and data
- Backup and Disaster Recovery: Ensure business continuity
- Support and Monitoring: Third-party security tools

6.1.1 Authorised Sub-Processors

| Sub-Processor | Purpose | Location | Standard | |---|---|---|---| | OpenProvider | Domain registration | Netherlands | GDPR-compliant | | eNom | Domain registration | USA | SCC in place | | Ascio Technologies | Domain registration | Denmark | GDPR-compliant | | Twcoms Domains | Domain registration | USA | SCC in place | | Stripe | Payment processing | USA/EU | PCI-DSS Level 1 | | PayPal | Payment processing | USA/EU | PCI-DSS compliant | | Google Cloud | Infrastructure | EU/US | Data Processing Agreement | | AWS | Backup and recovery | EU/US | Data Processing Agreement | | Cloudflare | CDN and security | Global | Data Processing Agreement |

6.1.2 Sub-Processor Requirements

All sub-processors must:

- Execute written Data Processing Agreement
- Comply with GDPR or equivalent protections
- Implement security measures equivalent to Domanenname
- Not engage further sub-processors without approval
- Maintain confidentiality of personal data

- Assist with data subject rights
- Notify of data breaches

6.1.3 Changes to Sub-Processors

Customer Right to Object:

- Domanenname provides 30 days’ notice of new sub-processors
- Customers may object in writing
- If objection not resolved, customer may terminate affected services
- No penalty for termination due to sub-processor change

6.2 International Data Transfers

6.2.1 Transfer Mechanisms

Personal data is transferred outside UK/EU to the following countries:

USA \(OpenProvider, eNom, Twcoms, Stripe, Google Cloud, AWS,) Tj ET BT /F1 11 T

- Mechanism: Standard Contractual Clauses \(SCC\)
- Status: Approved by relevant data protection authorities
- Agreement: Data Processing Agreements executed
- Safeguards: US cloud providers provide contractual guarantees

Denmark \(Ascio Technologies\)

- Mechanism: GDPR adequacy \(Denmark part of GDPR regime\)
- Status: No transfer issues; equivalent protections
- Safeguards: Full GDPR compliance

Netherlands \(OpenProvider\)

- Mechanism: GDPR adequacy \(Netherlands part of GDPR regime\)
- Status: No transfer issues; equivalent protections
- Safeguards: Full GDPR compliance

6.2.2 Supplementary Safeguards

For transfers to USA, Domanenname has implemented:

- Contractual Protections: Standard Contractual Clauses with binding force
- Transparency: US government access disclosed in Data Processing Agreements
- Technical Measures: Encryption during transmission and storage
- Consent: Customers informed of international transfers \(Privacy) Tj ET BT /F1

6.2.3 Customer Data Subject Rights

Data subjects have right to:

- Know data is transferred internationally
- Understand protections in place
- Request transfer restrictions \(where permitted\)
- Object to transfer \(where permitted by law\)

To Exercise Rights:

- Contact: privacy@domanenname.com
- Request: Information on transfers and protections

---

7. DATA BREACH AND INCIDENT RESPONSE

7.1 Data Breach Definition

A data breach is:

- Unauthorised or accidental access to personal data
- Unauthorised or accidental transmission of data
- Unauthorised or accidental alteration of data
- Unauthorised or accidental deletion of data
- Destruction or loss due to system failure
- Accidental loss of backups or archives

Not a breach:

- Authorised access or processing
- Access by lawful authority with warrant
- Encrypted data with secure keys \(if not compromised\)

7.2 Incident Response Procedure

Upon Discovery of Suspected Breach:

Step 1: Immediate Containment \(0-24 hours\)

- Immediately isolate affected systems
- Preserve evidence
- Assess scope of breach
- Identify affected personal data
- Stop further unauthorised access
- Document timeline and actions

Step 2: Assessment \(24-48 hours\)

- Determine which data was accessed
- Identify how long data was exposed

- Assess likelihood of unauthorised use
- Evaluate risk to data subjects
- Determine if notification required
- Document findings

Step 3: Customer Notification \(Immediate\)

- Email to customer within 24 hours of confirmed breach
- Details:
  - Nature of breach
  - Date/time discovered
  - Data affected
  - Number of individuals affected
  - Risk assessment
  - Actions taken
  - Recommended remediation
- Customer directed to contact privacy@domanenname.com

Step 4: Supervisory Authority Notification \(If Required\)

- Notify relevant data protection authority within 72 hours
- If high risk to data subjects
- Report must include:
  - Nature and scope of breach
  - Personal data concerned
  - Likely consequences
  - Measures taken or proposed
  - Data Protection Officer contact

Step 5: Data Subject Notification \(If Required\)

- Notify affected individuals within 72 hours of customer decision
- If high risk \(e.g., financial fraud likely\)
- Notification includes:
  - Nature of breach
  - Data affected
  - Risks to individual
  - Steps taken to remediate
  - Recommendations for individuals
  - Contact information

Step 6: Investigation and Remediation \(1-2 weeks\)

- Full root cause analysis
- Remediation of vulnerability

- Implementation of additional safeguards
- Customer updated regularly
- Post-incident review
- Documentation of incident and lessons learned

Step 7: Communication \(Ongoing\)

- Regular updates to customer
- Updates to supervisory authority if required
- Final incident report to customer
- Recommendations for future prevention

7.3 Notification Timeline

| Phase | Timeline | Action | |-------|----------|--------| | Discovery | Immediate | Incident team alerted | | Containment | 0-24 hours | Systems isolated | | Assessment | 24-48 hours | Scope determined | | Customer Notification | Within 24 hours | Email sent to customer | | Supervisory Authority | Within 72 hours \(if) Tj ET BT /F1 11 T

hours \(if required\) | Letters/emails sent |

7.4 Incident Record Keeping

Domanenname maintains records of:

- Date and time of incident
- Date and time of discovery
- Date and time of notification
- Description of personal data affected
- Number of data subjects affected
- Number of records affected
- Risk assessment conclusion
- Actions taken
- Lessons learned
- Incident investigation report

---

8. AUDIT AND COMPLIANCE

8.1 Audit Rights

Customer Right to Audit: Customers have right to:

- Request information about processing activities
- Request evidence of security measures
- Request audit reports \(upon reasonable notice\)

- Conduct audit of Domanenname systems \(with reasonable limitations\)
- Request certifications \(ISO 27001, SOC 2\)
- Request evidence of sub-processor compliance

Audit Request Process:

1. Email: compliance@domanenname.com
2. Specify: Audit scope, dates, systems involved
3. Scheduling: Within 30 days of request
4. Limitation: Max 1 audit per year \(unless breach or compliance) Tj ET BT /F1

5. Cost: Reasonable audits at no additional cost; extensive audits may incur reasonable fees

Third-Party Audits:

- Customer may appoint third-party auditor
- Subject to signed confidentiality agreement
- Domanenname provides reasonable cooperation
- Costs borne by customer

8.2 Compliance Certifications

Domanenname maintains:

- ISO 27001: Current certification \(annual audit\)
- SOC 2 Type II: Annual audit with report available to customers
- GDPR Compliance: Documented compliance with all requirements
- PCI-DSS: Payment card data security certification

Certificate Availability:

- Available to customers on request
- Provided under confidentiality agreement if requested
- Current copies maintained in compliance department

8.3 Annual Review

Domanenname conducts annual review of:

- Data protection practices and procedures
- Security controls effectiveness
- Sub-processor compliance
- International transfer safeguards
- Data minimisation practices
- Incident log and lessons learned
- This DPA compliance

---

9. CUSTOMER RESPONSIBILITIES

9.1 Customer Obligations

As Data Controller, customers are responsible for:

9.1.1 Legal Compliance

- Ensuring collection of personal data complies with law
- Obtaining necessary consents from data subjects
- Providing privacy notices to data subjects
- Complying with data subject access rights
- Complying with data subject erasure requests
- Complying with GDPR Articles 12-22 \(data subject rights\)

9.1.2 Processing Instructions

- Providing clear, written processing instructions
- Ensuring instructions comply with applicable law
- Notifying Domanenname of changes to instructions
- Approving Sub-Processors and transfers
- Reviewing and approving this DPA terms

9.1.3 Data Accuracy

- Ensuring personal data provided is accurate and complete
- Updating data when changed
- Ensuring authorisation to provide data
- Ensuring data does not violate third-party rights
- Ensuring data is not obtained through deception

9.1.4 Data Minimisation

- Collecting only necessary personal data
- Reviewing and deleting unnecessary data
- Instructing Domanenname to delete data when no longer needed
- Balancing data collection with privacy rights

9.2 Customer Cooperation

Customers must cooperate with:

- Providing processing instructions in writing
- Responding to Domanenname requests for information
- Assisting with data subject rights requests
- Assisting with audit and compliance activities
- Notifying of legal requests for data
- Sharing breach information promptly

9.3 Customer Support for Data Subject Rights

Customers must:

- Provide data subjects mechanism to exercise rights \(through) Tj ET BT /F1 11

- Respond to data subject requests
- Forward requests to Domanenname if unable to fulfill
- Cooperate with Domanenname in fulfilling data subject rights
- Not obstruct data subject exercises of rights

---

10. DATA RETENTION AND DELETION

10.1 Retention Periods

Personal data is retained for:

| Data Type | Retention | Reason | |---|---|---| | Active domain registrant data | Registration duration + 1 year | ICANN audit requirement | | Cancelled domain data | 1 year post-cancellation | Legal hold; dispute resolution | | Payment and billing data | 10 years | UK tax requirement | | Support communications | 24 months | Dispute resolution window | | Access logs | 12 months | Security and audit | | Failed login attempts | 6 months | Security analysis | | Active sessions | 24 hours after logout | Session management only | | Backup data | 30 days | Disaster recovery only |

10.2 Deletion Procedure

Upon Instruction to Delete:

1. Customer or data subject requests deletion
2. Assessment of legal retention requirements
3. If no legal hold: Data marked for deletion
4. Physical/cryptographic deletion within 30 days
5. Sub-processors notified of deletion requirement
6. Confirmation email to requester
7. Backup data deleted per backup retention policy

Exceptions to Deletion:

- Active domain registration \(must remain for ICANN\)
- Tax records \(legal 6-year requirement\)
- Ongoing legal proceedings
- Court orders or legal holds
- Regulatory requirements \(e.g., AML/CFT\)

10.3 Retention Exceptions

Data may be retained beyond normal period if:

- Legal Hold: Court order or litigation pending
- Law Enforcement: Investigation or prosecution pending
- Regulatory Requirement: Tax, compliance, or audit obligation
- Contractual Obligation: Customer contract requires retention

---

11. TERM AND TERMINATION

11.1 Duration of DPA

This DPA:

- Enters into force: Upon customer registration with Domanenname
- Continues: For duration of customer relationship
- Survives: Termination of Terms of Service \(for deletion/retention) Tj ET BT /

- Amended: As required by law or new GDPR requirements

11.2 Termination of Processing

Upon customer termination of service:

30-Day Transition Period:

1. Customer may request data export \(in portable format\)
2. Domanenname assists with data transfer to new processor
3. Data continues to be processed per instructions
4. Customer reviews and approves data deletion plan

Deletion Following Termination:

- Non-required data deleted within 30 days
- Backup data deleted per schedule \(max 30 days\)
- Sub-processors notified of service termination
- Confirmation of deletion provided to customer

Exceptions:

- Data required for legal/regulatory reasons retained per retention schedule
- Backup data retained per backup retention policy

11.3 Survival

The following obligations survive termination:

- Confidentiality obligations
- Security obligations \(during transition\)

- Data breach notification requirements
- Audit rights \(for past processing\)
- Record-keeping requirements

---

12. MODIFICATIONS AND UPDATES

12.1 GDPR Compliance Updates

Domanenname may update this DPA:

- To comply with new GDPR guidance
- To comply with new UK data protection law
- To reflect new security standards
- To add Sub-Processors
- To modify retention periods \(within reason\)

Notice Requirement:

- 30 days’ advance notice to all customers
- Email notification of changes
- Summary of changes provided
- Updated DPA available on website

Customer Right to Reject:

- Customers may reject material changes
- Rejection must be in writing within 30 days
- If rejected, customer may terminate service
- No penalty for termination due to DPA changes

12.2 Sub-Processor Changes

Changes to Sub-Processors require:

- 30 days’ advance notice
- Information about new Sub-Processor
- Security and compliance information provided
- Customer right to object \(see Section 6.1.3\)

---

13. DISPUTE RESOLUTION

13.1 Processing Disputes

If customer disputes Domanenname’s processing:

Process:

1. Customer contacts: privacy@domanenname.com

2. Dispute documented in writing
3. Domanenname investigates within 15 days
4. Response provided with explanation and remediation
5. If unresolved, escalation to DPO and management

13.2 Supervisory Authority Escalation

If dispute unresolved:

- Customer may file complaint with data protection authority
- UK: Information Commissioner’s Office \(ICO\)
- EU: Customer’s national data protection authority
- Domanenname will cooperate with authority investigation

13.3 Litigation and Arbitration

Final disputes may be resolved through:

- Civil court proceedings \(Courts of England and Wales\)
- Arbitration \(if customer agrees\)
- Alternative dispute resolution/mediation

---

14. GENERAL PROVISIONS

14.1 Governing Law

This DPA is governed by:

- Primary: UK General Data Protection Regulation \(UK GDPR\)
- Supplementary: Data Protection Act 2018
- Interpretation: Laws of England and Wales

14.2 Entire Agreement

This DPA, together with:

- Domanenname Terms of Service
- Domanenname Privacy Policy
- This Acceptable Use Policy
- Refund and Cancellation Policy

Constitutes the entire agreement regarding personal data processing.

14.3 Conflict Resolution

If conflict between this DPA and other agreements:

- GDPR requirements take precedence
- Most protective interpretation adopted
- Domanenname and customer will reconcile in writing

14.4 No Waiver

Failure to enforce any provision:

- Does not constitute waiver of the provision
- Does not limit future enforcement rights
- Does not affect other provisions

14.5 Severability

If any provision is invalid:

- Provision severed
- Other provisions remain in effect
- Invalid provision replaced with valid equivalent

---

15. CONTACT INFORMATION

For DPA Questions:

- Email: privacy@domanenname.com

For Data Subject Access Requests:

- Email: privacy@domanenname.com
- Web Form: https://domanenname.com/privacy-request
- Response Time: 30 days

For Data Protection Officer:

- Email: dpo@domanenname.com

For Data Breach Notifications:

- Email: privacy@domanenname.com
- Urgent: https://domanenname.com/breach-report

For Audit Requests:

- Email: compliance@domanenname.com

For Supervisory Authority Complaints:

- UK: Information Commissioner’s Office
  - Website: https://ico.org.uk
  - Phone: 0303 123 1113
  - Address: Water Lane, Wigan, WN3 5DJ
- EU: Your national data protection authority

---

16. APPENDICES

Appendix A: Sub-Processors List

[See Section 6.1.1 - Authorised Sub-Processors table]

Appendix B: Standard Contractual Clauses

For international transfers to USA:

- SCC Module One \(Customer to Domanenname\)
- SCC Module Three \(Domanenname to Sub-Processors\)
- Available upon request from compliance@domanenname.com

Appendix C: Data Processing Record

Domanenname maintains Records of Processing Activities \(RPA\) per GDPR Article 30:

- Available for customer review upon request
- Updated annually
- Provided under confidentiality agreement

Appendix D: Security Documentation

- ISO 27001 Certificate \(current\)
- SOC 2 Type II Report \(annual\)
- Penetration Testing Reports \(annual, non-public\)
- Data Protection Impact Assessment

Version: 1.0 Last Updated: 18th May 2026 Next Review: 31st December 2026 Effective Date: 18th May 2026

Approved by: CRISALEO LIMITED DPO & Compliance Team

Important Notice:

This Data Processing Agreement is required by law \(UK GDPR, EU GDPR,) Tj ET BT

processing personal data. By registering a domain with Domanenname, you acknowledge that:

1. You have reviewed this DPA
2. You understand Domanenname’s role as Data Processor
3. You understand your obligations as Data Controller
4. You consent to processing per this DPA
5. You accept international data transfers as described

If you do not accept these terms, you may not use Domanenname services. For questions or concerns, contact privacy@domanenname.com immediately.