**Cybersecurity Templates**

**Data Transfer Policy**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Data Transfer Policy** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Organisation:** |  | **Effective Date:** |  |
| **Owner:** |  | **Approved By:** |  |

Contents

[1. Purpose 4](#_Toc207055897)

[2. Scope 4](#_Toc207055898)

[3. Definitions 4](#_Toc207055899)

[4. Policy Principles 5](#_Toc207055900)

[5. Governance & Roles 5](#_Toc207055901)

[6. Legal Bases & Cross-Border Mechanisms 5](#_Toc207055902)

[7. When This Policy Applies (Transfer Triggers) 6](#_Toc207055903)

[8. Pre‑Transfer Assessment 6](#_Toc207055904)

[9. Approved Transfer Methods & Security Controls 6](#_Toc207055905)

[10. Vendor & Sub‑Processor Management 7](#_Toc207055906)

[11. Transfer Execution Workflow 7](#_Toc207055907)

[12. Records & Evidence 7](#_Toc207055908)

[13. Data Subject Rights & Transparency 7](#_Toc207055909)

[14. Incidents & Breach Notification 8](#_Toc207055910)

[15. Training & Awareness 8](#_Toc207055911)

[16. Monitoring, Audit & KPIs 8](#_Toc207055912)

[17. Exceptions 8](#_Toc207055913)

[18. Enforcement 8](#_Toc207055914)

[19. Review 8](#_Toc207055915)

[Annex A — Transfer Impact Assessment (TIA) — Short Form 9](#_Toc207055916)

[Annex B — Transfer Register (Template) 10](#_Toc207055917)

[Annex C — Security Controls (TOMs) Checklist 10](#_Toc207055918)

[Annex D — Mechanism Selection Guide (Quick Reference) 11](#_Toc207055919)

[Annex E — Approved Transfer Channels & Config Standards 11](#_Toc207055920)

[Annex F — Government/Law‑Enforcement Requests 11](#_Toc207055921)

[Annex G — Contacts & Responsibilities 11](#_Toc207055922)

[Acknowledgement 11](#_Toc207055923)

# 1. Purpose

This policy outlines the mandatory requirements for transferring data to third parties or across borders, ensuring the confidentiality, integrity, availability, and lawful processing of personal and confidential information.

# 2. Scope

Applies to:

* All business units, subsidiaries, and affiliates of [Organisation Name].
* All personnel (employees, contractors, temporary staff) and third parties handling transfers on our behalf.
* All transfers of **Personal Data**, **Special Category/Sensitive Data**, and **Confidential Business Data**, whether manual or electronic, domestic or cross-border.

# 3. Definitions

* **Personal Data:** Information relating to an identified or identifiable natural person.
* **Special Category Data:** Personal data revealing racial/ethnic origin, political opinions, religious beliefs, trade union membership, genetic, biometric (unique ID), health, sex life, or sexual orientation.
* **Processing:** Any operation performed on data (e.g., collection, storage, use, disclosure, deletion).
* **Transfer:** Disclosure or remote access of data to another entity or location, including cloud hosting outside the originating jurisdiction.
* **Controller / Processor:** Roles per applicable data protection laws (e.g., GDPR/UK GDPR).
* **TIA:** Transfer Impact Assessment evaluating cross-border risks and safeguards.
* **TOMs:** Technical and Organisational Measures (security controls).
* **Adequacy:** Decision by a regulator recognising another jurisdiction ensures an essentially equivalent level of protection.
* **SCCs/IDTA/Addendum:** Standard contractual mechanisms for cross-border transfers.

# 4. Policy Principles

1. **Lawfulness, Fairness, Transparency:** All transfers must have a lawful basis and be communicated in relevant notices.
2. **Purpose Limitation:** Transfer only for specified, explicit purposes.
3. **Data Minimisation:** Share the minimum data necessary (fields, records, retention).
4. **Accuracy:** Verify data before transfer; correct inaccuracies without delay.
5. **Storage Limitation:** Apply documented retention schedules; delete or anonymise when no longer required.
6. **Security:** Apply proportionate TOMs (encryption, access control, logging, DLP).
7. **Accountability:** Maintain evidence of assessments, approvals, and safeguards.
8. **Onward Transfers:** Prohibit or strictly control; require equivalent protections and prior authorisation.

# 5. Governance & Roles

* **Executive Sponsor:** Ensures resources and enforcement.
* **Data Protection Officer/Privacy Lead:** Advises on lawfulness, TIAs/DPIAs, and regulatory engagement.
* **Information Security Lead:** Defines TOMs; approves secure channels and configurations.
* **Procurement/Vendor Management:** Ensures contractual safeguards with processors/sub‑processors.
* **System/Data Owners:** Classify datasets; approve transfer requests; ensure data quality.
* **Requestor (Project/Team):** Completes TIA/Transfer Register entries and follows this policy.
* **Audit/Compliance:** Monitors adherence and reports issues.

# 6. Legal Bases & Cross-Border Mechanisms

* Identify and record the **lawful basis** (e.g., contract, legal obligation, legitimate interests, consent, vital interests).
* For cross-border transfers, use this hierarchy:

1. **Adequacy** (where available);
2. **Appropriate Safeguards** (e.g., SCCs, UK IDTA/Addendum, Binding Corporate Rules, approved codes/certifications);
3. **Derogations** (exceptional, one-off scenarios with strengthened safeguards and documentation).

* Conduct a **TIA** for all non-adequacy routes and when required by law or risk level.

# 7. When This Policy Applies (Transfer Triggers)

* Sharing data with external partners, vendors, or affiliates.
* Hosting/support by providers who can access data from other countries.
* Remote access to in-scope data from outside the originating jurisdiction.
* Publishing data to shared repositories or collaboration tools.
* Physical media shipments (USB, disk) or paper records leaving premises.

# 8. Pre‑Transfer Assessment

Before any transfer, the Requestor must:

* **Classify Data:** [Public / Internal / Confidential / Highly Confidential; mark personal vs. special category].
* **Define Purpose & Necessity:** Why is transfer required? Consider alternatives (aggregation, tokenisation).
* **Identify Roles:** Controller–Controller or Controller–Processor (and any sub-processors).
* **Recipient Due Diligence:** Security posture, certifications, audit reports, incident history, sub-processing.
* **Jurisdictional Risk:** Local laws, government access risk, redress, and enforcement.
* **Safeguards:** Contractual (SCCs/IDTA/BCRs), technical (encryption, key management), organisational (policies, training).
* **Residual Risk & Sign‑off:** DPO/Privacy, Security, and Data Owner approvals based on risk rating.
* **DPIA Linkage:** If high risk to individuals, conduct/attach DPIA.

# 9. Approved Transfer Methods & Security Controls

Transfers must use an approved method with mandated TOMs:

* **Secure File Transfer (SFTP/FTPS/Managed file gateways):** Enforce strong ciphers, mutual auth where feasible, IP allow‑listing.
* **HTTPS APIs:** TLS 1.2+; token‑based auth; rate limiting; payload encryption if sensitive.
* **Email (exceptional use only):** Mandatory message/file encryption; no bulk special category data via email.
* **Approved Cloud Storage:** Server-side encryption at rest; customer-managed keys for highly sensitive data; restricted links; lifecycle/retention rules.
* **Portable Media:** Discouraged; if unavoidable, encrypt with AES‑256, tamper-evident packaging, and chain‑of‑custody logs.
* **Data Format Controls:** Pseudonymise where possible; apply field-level minimisation and masking.
* **Access Control:** Least privilege, MFA, time-bound access, just-in-time provisioning.
* **Monitoring:** Transfer logging (who/what/when/where), DLP, anomaly alerts, reconciliation checks.

# 10. Vendor & Sub‑Processor Management

* Contracts must include data protection terms, security obligations, audit rights, breach notification timelines, assistance with rights requests, and conditions for sub-processors.
* Sub-processors require prior written authorisation and equivalent protections.
* Maintain an up-to-date list of authorised processors/sub-processors.

# 11. Transfer Execution Workflow

1. Submit **Transfer Request** and draft **TIA**.
2. Validate data mapping, purpose, roles, and mechanism (Adequacy/Safeguard/Derogation).
3. Obtain **contractual safeguards** (e.g., SCCs/IDTA) executed by Legal/Procurement.
4. Configure **approved method** and TOMs; test on sample/minimised dataset.
5. Record in **Transfer Register** (Annex B).
6. Execute transfer; monitor logs and reconcile receipt.
7. Store artefacts (contract, TIA, testing evidence, approvals) in the central repository.

# 12. Records & Evidence

Maintain: TIAs, DPIAs, contracts, approvals, logs, inventories, sub-processor lists, training records, and audit evidence for at least **[X years]** or as required by law.

# 13. Data Subject Rights & Transparency

* Ensure appropriate notices are in place and accessible.
* Provide reasonable assistance to respond to requests (access, rectification, deletion, restriction, portability, objection).
* Record all requests and responses in the **Rights Request Register**.

# 14. Incidents & Breach Notification

* Suspected or actual incidents must be reported to [Security Operations / DPO] **immediately** via [channel].
* Contain, assess impact, and notify regulators/data subjects as required by law and contracts.
* Keep an incident log (timeline, scope, measures taken, lessons learned).

# 15. Training & Awareness

Mandatory onboarding and annual training covering data transfer risks, secure methods, and escalation paths. Role-based training for high-risk teams (engineering, procurement, analytics).

# 16. Monitoring, Audit & KPIs

* Periodic reviews of the Transfer Register, sub-processor list, and TOM effectiveness.
* KPIs: % transfers with TIAs, time to complete approvals, DLP incident rate, remediation closure time.
* Independent/internal audits at least annually.

# 17. Exceptions

Exceptions must be rare, risk-assessed, time-limited, and approved by [DPO/Privacy Lead] and [CISO/Security Lead]. Record in the **Exceptions Log** with compensating controls.

# 18. Enforcement

Breaches of this policy may result in disciplinary action, up to and including termination of employment/contract, and may trigger contractual or legal remedies.

# 19. Review

This policy is reviewed at least annually or upon material changes to law, risk, services, or jurisdictions.

# Annex A — Transfer Impact Assessment (TIA) — Short Form

**Complete for each non-adequacy or high-risk transfer. Attach DPIA if required.**

**A. Overview**

* Requestor / Business Owner: [Name, Role]
* System / Dataset: [Name/ID]
* Purpose of Transfer: [Describe]
* Data Subjects & Categories: [Employees/Customers/End‑users; list fields]
* Sensitivity: [Personal / Special Category / Confidential Business / Mixed]
* Volume/Frequency: [One‑off / Recurring (daily/weekly/monthly)]

**B. Roles & Parties**

* Exporter Role: [Controller/Processor]
* Importer Role: [Controller/Processor]
* Recipient Entity & Country: [Name, Country]
* Sub‑processors (if any): [List or “None”]

**C. Legal Mechanism**

* Adequacy: [Yes/No; country]
* Safeguard: [SCCs / UK IDTA/Addendum / BCRs / Certification]
* Additional Safeguards: [Encryption at rest/in transit; E2EE; pseudonymisation; split‑processing; key split]

**D. Local Law & Access Risks**

* Summary of potential government access and redress in the recipient country: [Describe]
* Likelihood/impact assessment: [Low/Medium/High]
* Mitigations: [Technical, contractual, organisational]

**E. Data Minimisation & Security**

* Fields shared (include/exclude): [List]
* Pseudonymisation/tokenisation: [Yes/No; method]
* Encryption in transit/at rest: [Protocols, key management]
* Access controls: [MFA, least privilege, time-bound]
* Logging/Monitoring: [Describe]

**F. Residual Risk & Decision**

* Residual Risk: [Low/Medium/High]
* Decision: [Proceed / Proceed with conditions / Do not proceed]
* Approvals:
* DPO/Privacy: [Name, Date, Signature]
* Security: [Name, Date, Signature]
* Data Owner: [Name, Date, Signature]

# Annex B — Transfer Register (Template)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Dataset/  System | Purpose | Exporter  Role | Importer & Country | Legal  Mechanism | TIA Ref | TOMs Summary | Start Date | Review Date |
| [#] | [e.g., CRM Contacts] | [Support] | [Controller] | [Vendor A, US] | [SCCs + E2EE] | [TIA‑  001] | [TLS1.2+, KMS, MFA] |  |  |

# Annex C — Security Controls (TOMs) Checklist

**Access & Identity**

* Unique IDs; MFA for administrators and remote access.
* Role‑based access; least privilege; periodic reviews.

**Encryption & Key Management**

* TLS 1.2+ for transit; strong ciphers.
* Encryption at rest with [AES‑256/Platform default].
* Keys stored in [HSM/KMS]; restricted access; rotation policy.

**Data Handling**

* Pseudonymisation/minimisation before transfer.
* No special category data via email; approved channels only.
* Secure deletion (policy + verification).

**Monitoring & Resilience**

* Transfer logging with tamper‑evidence and retention.
* DLP and anomaly alerts on export paths.
* Backups tested; disaster recovery objectives defined.

**Physical & Organisational**

* Facility security; vetted personnel; confidentiality undertakings.
* Secure configuration baseline; patching SLAs.
* Incident response plan covering cross‑border scenarios.

# Annex D — Mechanism Selection Guide (Quick Reference)

1. **Adequacy** available → proceed with standard contract + TOMs.
2. **No adequacy** → use **SCCs/IDTA/Addendum** (controller–controller/processor module as applicable) + **TIA** + additional safeguards.
3. **Group transfers** → consider **BCRs** (where approved).
4. **Derogations** (explicit consent, contract performance, public interest, legal claims, vital interests) → last resort; document rationale and limitations.

# Annex E — Approved Transfer Channels & Config Standards

* **SFTP/Managed Gateway:** Enforce strong algorithms, time‑bound accounts, IP allow‑listing.
* **HTTPS API:** OAuth2/OpenID Connect; rate limits; schema validation; error redaction.
* **Email Encryption:** Use [gateway/tool]; auto‑encrypt by policy/labels; prohibit forwarding.
* **Cloud Object Storage:** Private endpoints/VPC peering; server‑side encryption; bucket policies; lifecycle rules.
* **Portable Media:** Only with executive approval; full‑disk encryption; chain‑of‑custody; immediate deletion post‑ingest.

# Annex F — Government/Law‑Enforcement Requests

* Route all requests to **Legal** and **DPO** immediately.
* Verify jurisdiction and legal validity; challenge unlawful or over‑broad demands.
* Notify exporter and affected individuals where permitted; document decision and disclosures.

# Annex G — Contacts & Responsibilities

* **DPO/Privacy:** [Name, email, phone]
* **Information Security:** [Name, email, phone]
* **Vendor Management/Procurement:** [Name, email, phone]
* **Incident Reporting (24/7):** [Channel/email/phone]
* **Records Repository:** [System/URL/Path]

# Acknowledgement

I acknowledge that I have read and understand this Data Transfer Policy and agree to comply with its requirements.  
**Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Role:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_\_\_\_