KAT-C CONSULTING

2025 DSA Checklist for Business Owners

Created by KAT-C Data Privacy Business and Consultant Inc.

As data protection regulations evolve, it is critical for businesses to have a robust Data Sharing Agreement (DSA) in place when exchanging data with third parties, partners, or vendors. This 2025 DSA Checklist is designed to help business owners ensure their agreements remain compliant, secure, and enforceable.

DSA Checklist – Essential Components

1. Parties and Their Roles

With increasingly complex cross-border data transfers (especially under GDPR adequacy rules and post-CCPA amendments), precise role definition helps avoid liability disputes and ensures regulatory clarity.

- ☐ **Define all entities involved:** Clearly list every organization or individual participating in the data sharing.
- ☐ **Assign roles:**
  - **Data Controller:** Determines the purpose and means of processing.
  - **Data Processor:** Processes data on behalf of the controller.
  - **Joint Controllers:** Share decision-making responsibilities.
- ☐ Include subcontractors and affiliates where applicable.

Why it matters: Misidentifying roles can result in **liability confusion** during audits or breaches.

2. Purpose and Scope of Sharing

Regulators now require greater transparency around secondary data use, especially with AI-driven processing and profiling.

- [ ] **Describe the purpose:** Clearly state why data is being shared (e.g., marketing, analytics, service delivery).
- [ ] **Specify data types:** Identify what categories of data are involved (personal, sensitive, financial, etc.).
- [ ] **Set use limitations:** Restrict data use to the agreed purposes; prohibit repurposing without explicit consent.
- [ ] Specify **who may access the data** and for what functions.
- [ ] Explicitly prohibit **unauthorized secondary use** (e.g., resale, AI training, profiling).

Why it matters: Overly vague DSAs invite **regulatory penalties** and create loopholes for misuse.

3. Legal Basis for Processing

Increasing scrutiny on **automated decision-making** means DSAs must include **algorithmic fairness and transparency clauses**.

- [ ] **Identify lawful basis:** Reference the applicable legal grounds (e.g., GDPR Article 6, CCPA/CPRA, or other regional privacy acts).
- [ ] **Ensure explicit consent:** Obtain and document consent where required, especially for sensitive data.
- [ ] **Address cross-border data transfers:** Standard Contractual Clauses (SCCs), Binding Corporate Rules, or adequacy decisions.
- [ ] Confirm compliance with **new AI/data laws** (e.g., EU AI Act).

Why it matters: Processing without a valid legal basis = **illegal data processing**.

4. Security Controls

With increased cyberattacks targeting small businesses and supply chains, agreements must reflect zero-trust architecture and incident readiness.

- [ ] **Encryption:** Require encryption of data both in transit and at rest.
- [ ] **Access controls:** Limit access to authorized personnel only, using role-based access control.
- [ ] **Testing and audits:** Mandate regular penetration testing and security audits by both parties.
- [ ] **Security certifications:** Require up-to-date certifications (e.g., ISO 27001).
- [ ] Include obligations for **employee training** on data security.

Why it matters: Security failures cause reputational damage and fines.

5. Retention and Disposal Terms

Newer laws emphasize data minimization and storage limitation; retaining data longer than necessary can trigger penalties.

- [ ] **Define retention periods:** Set clear timelines for how long data will be retained, aligned with business needs and compliance requirements.
- [ ] **Secure disposal:** Require secure deletion or anonymization of data once it is no longer needed.
- [ ] **Deletion requests:** Document procedures for responding to data subject deletion requests.
- [ ] Document **data subject rights** (erasure, portability).

Why it matters: Retaining data longer than necessary increases **legal risk and storage costs**.

6. Breach Reporting Process

Stricter reporting obligations under laws like GDPR, CPRA, and APPI (Japan) mean failure to notify regulators and customers in time can result in heavy fines and reputational damage.

- [ ] **Reporting timeline:** Establish a clear timeline for reporting breaches (typically within 24–72 hours).
- [ ] **Incident contacts:** Define responsible contacts at each party for incident escalation.
- [ ] **Incident reports:** Require detailed reports including root cause analysis and mitigation steps.
- [ ] Define responsibility for **regulator and customer notifications**.

Why it matters: Delayed reporting = **higher penalties** and **loss of trust**.

7. Dispute Resolution Steps

With more cross-border data sharing, clarity on dispute resolution is essential to avoid costly legal battles.

- [ ] **Escalation paths:** Outline steps for resolving disputes (negotiation → mediation → arbitration → litigation).
- [ ] **Governing law and jurisdiction:** Specify which laws apply and where disputes will be resolved.
- [ ] Include **liability caps** and **indemnification clauses**.
- [ ] Define process for **contract termination** in case of unresolved disputes.

Why it matters: Clear dispute resolution prevents **lengthy, expensive lawsuits**.

Download and Use

This checklist is provided as a free resource by KAT-C Data Privacy Business and Consultant Inc. for business owners seeking to strengthen their data sharing practices in 2025. Use this as a guide to review, draft, or update your Data Sharing Agreements to ensure compliance, security, and business continuity.

For further guidance or customized DSA templates, contact KAT-C Data Privacy Business and Consultant Inc. Visit www.katcdataprivacy.com