

# Utilitarian Data Processing Agreement

Version 2.0

Last updated: 25 February 2026

*Effective for all accounts created or continued on or after this date.*

## About this DPA

This Data Processing Agreement (“DPA”) is incorporated into and forms part of the Utilitarian Platform Terms of Service (“Terms”) between your organisation (“Client”, “you”, “Controller”) and the applicable Utilitarian entity (“Utilitarian”, “we”, “Processor”).

This DPA applies whenever Utilitarian processes personal data on behalf of Client in providing the Platform. It satisfies the requirements of Article 28 of the EU General Data Protection Regulation (Regulation (EU) 2016/679) (“GDPR”) and, where applicable, the UK GDPR and the Australian Privacy Act 1988 (Cth).

By accepting the Terms, you also accept this DPA.

## 1. Roles and Scope

### 1.1 Controller and Processor

**Client is the data controller** — Client determines the purposes and means of processing personal data collected through the Platform.

**Utilitarian is the data processor** — Utilitarian processes personal data on behalf of Client to provide the Platform and related services.

### 1.2 Independent controller processing

For a limited set of data, Utilitarian acts as an independent data controller. This includes:

- billing and commercial contact data necessary for account management;
- security logs, authentication logs, and system administration data necessary to secure and operate the Platform; and
- aggregated, de-identified insights that do not identify any individual.

Utilitarian processes this data in accordance with its Privacy Policy, available at <https://www.utilitarian.world/hubfs/Privacy%20Policy%20Harmonised%20v1.0%20AUG%202025.pdf>.

### 1.3 Scope

This DPA applies to all personal data processed by Utilitarian on behalf of Client through the Platform, as described in **Annex 1 (Processing Details)**.

## 2. Processing Instructions

### 2.1 Documented instructions

Utilitarian will process personal data only on documented instructions from Client, including:

- (a) the instructions set out in these Terms and this DPA;
- (b) the processing inherent in providing the Platform services as described in the Terms; and
- (c) any additional documented instructions agreed in writing (including via Service Order).

## **2.2 Notification of conflicting instructions**

If Utilitarian reasonably believes that a processing instruction from Client violates applicable data protection law, Utilitarian will inform Client before carrying out that instruction, unless prohibited from doing so by law.

## **2.3 No other processing**

Utilitarian will not process personal data for any purpose other than providing the Platform services and complying with applicable law, unless Client provides documented instructions to the contrary.

## **3. Confidentiality**

Utilitarian ensures that all persons authorised to process personal data under this DPA:

- (a) are bound by appropriate confidentiality obligations (whether contractual or statutory); and
- (b) process personal data only in accordance with Client's documented instructions and this DPA.

## **4. Security Measures**

### **4.1 Appropriate measures**

Utilitarian implements and maintains appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing.

### **4.2 Specific measures**

Utilitarian's security measures include, at minimum:

#### **Access control:**

- Named user accounts (no shared accounts)
- Role-based access control (RBAC) with least-privilege design
- Multi-factor authentication for administrative accounts
- Account provisioning/deprovisioning processes and periodic access reviews

#### **Data protection:**

- Encryption in transit (TLS) for all platform traffic
- Encryption at rest for stored uploads and databases

- Logical tenant separation between client environments

#### **Logging and monitoring:**

- Authentication and admin action logging
- Image access logging (view events, denied access events)
- Export event logging
- Monitoring and alerting for anomalous access patterns

#### **Vulnerability management:**

- Regular patching of operating systems and dependencies
- Vulnerability scanning on a regular cadence
- Critical vulnerability remediation within 14 days (or faster where warranted)

#### **Backup and recovery:**

- Regular backups of core operational data and configurations
- Tested restore procedures

#### **Incident response:**

- Documented incident response plan
- Defined escalation contacts and procedures

### **4.3 Programme Partner access controls**

Where Client uses the Platform in connection with a Programme Partner, Utilitarian implements technical controls to ensure that Programme Partner users:

- cannot access customer personal data (email addresses and other direct identifiers);
- cannot access quarantined images;
- can view approved images only within the Platform interface, with no download, export, or scraping capability; and
- have their access to the Platform audit-logged.

## **5. Sub-processors**

### **5.1 Authorisation**

Client provides general authorisation for Utilitarian to engage sub-processors to assist in providing the Platform, subject to the requirements of this Section 5.

### **5.2 Sub-processor list**

Utilitarian maintains a current list of sub-processors at <https://www.utilitarian.world/legal/sub-processors> (“Sub-processor List”). The Sub-processor List identifies each sub-processor, its location, and the processing it performs.

### **5.3 Changes to sub-processors**

Before engaging a new sub-processor or replacing an existing sub-processor, Utilitarian will:

- (a) update the Sub-processor List at least 30 days before the new sub-processor begins processing personal data; and
- (b) notify Client of the change by email to the account admin address.

#### **5.4 Objection right**

If Client has a reasonable, data-protection-related objection to a new sub-processor, Client may notify Utilitarian in writing within 15 days of receiving notice. The parties will discuss the objection in good faith. If the objection cannot be resolved within 30 days, Client may terminate the affected Service Order without penalty by giving written notice.

#### **5.5 Sub-processor obligations**

Utilitarian ensures that each sub-processor is bound by data protection obligations no less protective than those in this DPA. Utilitarian remains fully liable to Client for the acts and omissions of its sub-processors.

#### **5.6 EU/EEA sub-processors**

For personal data of data subjects in the EEA, Utilitarian will use EU/EEA-based sub-processors only, unless otherwise agreed in writing with Client and subject to appropriate safeguards (see Section 9).

### **6. Data Subject Rights**

#### **6.1 Assistance**

Utilitarian will provide reasonable assistance to Client in responding to requests from data subjects to exercise their rights under applicable data protection law (including rights of access, rectification, erasure, restriction, portability, and objection), taking into account the nature of processing and the information available to Utilitarian.

#### **6.2 Notification**

If Utilitarian receives a request directly from a data subject, Utilitarian will promptly redirect the data subject to Client (unless prohibited by law) and notify Client of the request.

#### **6.3 Costs**

Assistance under this Section 6 is provided at no additional charge for routine requests. Utilitarian may charge reasonable costs for requests that are manifestly excessive, repetitive, or require significant manual effort, subject to prior agreement.

### **7. Personal Data Breaches**

#### **7.1 Notification**

Utilitarian will notify Client without undue delay, and in any event within **48 hours**, after becoming aware of a personal data breach affecting Client's personal data.

## **7.2 Content of notification**

The notification will include, to the extent available:

- (a) a description of the nature of the breach, including the categories and approximate number of data subjects and records affected;
- (b) the likely consequences of the breach;
- (c) the measures taken or proposed to address the breach and mitigate its effects; and
- (d) the contact point for further information.

Where not all information is available at the time of initial notification, Utilitarian will provide information in phases without undue delay.

## **7.3 Cooperation**

Utilitarian will provide reasonable cooperation and assistance to Client in relation to Client's breach assessment and notification obligations under applicable law.

## **7.4 No assessment of risk**

Notification under this Section 7 is not an acknowledgement of fault or liability. Client is responsible for determining whether a breach requires notification to supervisory authorities or data subjects.

## **8. Audits**

### **8.1 Information**

Upon reasonable request, Utilitarian will provide Client with information necessary to demonstrate compliance with this DPA, including relevant certifications, audit reports, or summaries of security measures.

### **8.2 Audit rights**

Client (or a qualified third-party auditor appointed by Client) may conduct an audit of Utilitarian's processing activities under this DPA, subject to the following conditions:

- (a) Client provides at least 30 days' written notice;
- (b) audits are conducted during business hours and no more than once per 12-month period (unless required by a supervisory authority or in response to a specific breach);
- (c) the auditor is bound by appropriate confidentiality obligations;
- (d) the audit scope is limited to Utilitarian's processing of Client's personal data;
- (e) Client bears its own audit costs; and
- (f) audits are conducted in a manner that does not unreasonably disrupt Utilitarian's operations or compromise the security or confidentiality of other clients' data.

### **8.3 Third-party reports**

Where Utilitarian holds relevant third-party certifications or audit reports (such as SOC 2 or ISO 27001), Utilitarian may provide these in lieu of a direct audit, provided they reasonably address Client's audit objectives.

## **9. International Transfers**

### **9.1 EU/EEA hosting**

For personal data of data subjects in the EEA, Utilitarian hosts and processes data in the EEA, unless otherwise agreed in writing with Client.

### **9.2 Transfer safeguards**

If any transfer of personal data outside the EEA is agreed, Utilitarian will ensure appropriate safeguards are in place, including:

- (a) the EU Standard Contractual Clauses (Commission Decision 2021/914), which are incorporated into this DPA by reference and will apply in the configuration set out in Annex 2; or
- (b) transfer to a jurisdiction with an adequate level of protection as determined by the European Commission; or
- (c) other safeguards approved under applicable data protection law.

### **9.3 Australian data**

For personal data subject to the Australian Privacy Act, Utilitarian will comply with Australian Privacy Principle 8 (cross-border disclosure) and will ensure that any overseas recipient of personal data is bound by obligations substantially similar to the APPs.

## **10. Return and Deletion**

### **10.1 On termination**

Upon termination or expiry of the Terms:

- (a) Utilitarian will, at Client's written request, return Client's personal data in a commonly used, machine-readable format, or delete it. Client must make this request within 30 days of termination.
- (b) If no request is received within 30 days, Utilitarian will delete Client's personal data, except where retention is required by applicable law.
- (c) Deletion of personal data (including from backups) will be completed within 90 days of termination, except where retention is required by law.

### **10.2 Retention rules**

Specific retention periods apply:

- Approved Images: retained for the term of services plus 6 months, then deleted or de-identified.

- Quarantined Images: retained for 14 days after screening decision (standard), or until closure plus 30 days if a special request is initiated, then deleted.
- Telemetry/Event Data: retained for the term of services plus 6 months, then deleted or de-identified.
- Audit logs: retained for 24 months, then deleted.

**10.3 Certification**

On request, Utilitarian will provide written confirmation that deletion has been completed.

**11. Cooperation**

**11.1 Data Protection Impact Assessments**

Utilitarian will provide reasonable assistance to Client in conducting data protection impact assessments and prior consultations with supervisory authorities, where required by applicable law and to the extent the assessment relates to Utilitarian’s processing.

**11.2 Regulatory inquiries**

Utilitarian will cooperate with Client in responding to inquiries from data protection supervisory authorities relating to the processing of Client’s personal data under this DPA.

**12. Liability**

Liability under this DPA is governed by the liability provisions of the Terms.

**13. Term**

This DPA is effective for as long as Utilitarian processes personal data on behalf of Client. It survives termination of the Terms to the extent necessary to govern any retained personal data.

**14. Updates to this DPA**

This DPA may be updated in accordance with the update mechanism in Section 14 of the Terms. Material changes to this DPA (including changes to security measures, sub-processor provisions, or international transfer mechanisms) will be notified at least 30 days in advance.

**15. Governing Law**

This DPA is governed by the same law that applies to the Terms.

**Annex 1 — Processing Details**

Item	Detail
Subject matter	Processing of personal data to provide the Utilitarian Platform and related services

Duration	For the term of the Terms, plus any applicable retention period
Nature and purpose	Hosting, storage, AI-based image screening and classification, product/brand recognition, customer engagement (email capture, discount issuance), reporting and analytics, programme management
Categories of data subjects	End-customers participating in take-back/recycling programmes; Client's authorised users (staff, administrators)
Categories of personal data	Customer photo submissions (product images) and related metadata; customer email addresses (where collected); store and campaign details; technical data (IP address, device/browser information, approximate location); Client user account data (names, business email addresses, roles, permissions)
Special category data	Not intentionally processed. May occur incidentally through customer uploads (e.g., an upload containing a face or identity document), which is handled through the automated screening and quarantine workflow
Processor obligations	As set out in this DPA

## Annex 2 — Standard Contractual Clauses

Where personal data is transferred outside the EEA and Standard Contractual Clauses apply:

- Module Two (Controller to Processor) applies where Client is the data exporter and Utilitarian is the data importer.
- Clause 7 (Docking clause): included.
- Clause 9 (Sub-processors): Option 2 (General written authorisation) applies, with the notification and objection mechanism set out in Section 5 of this DPA.
- Clause 13 (Supervision): The supervisory authority of the EU Member State in which the data exporter is established, or — where the data exporter is not established in the EU — the supervisory authority of the Member State in which the data exporter's EU representative is established, will act as competent supervisory authority.
- Clause 17 (Governing law): The law of the Netherlands.
- Clause 18 (Forum): The courts of Amsterdam, the Netherlands.

The parties agree that the technical and organisational measures set out in Section 4 of this DPA satisfy the requirements of Annex II to the Standard Contractual Clauses.

## Annex 3 — Sub-processor List

A current list of sub-processors is maintained at: <https://www.utilitarian.world/legal/sub-processors>

This list is updated at least 30 days before any new sub-processor begins processing personal data. Changes are notified by email to account administrators.

*To subscribe to sub-processor change notifications, contact [privacy@utilitarian.world](mailto:privacy@utilitarian.world).*

**Utilitarian B.V. — Schiedamse Vest 154, 3011 BH Rotterdam (KVK 97343927)**

**Utilitarian Pty Ltd — ABN 89 655 178 402**

*Questions about this DPA: [privacy@utilitarian.world](mailto:privacy@utilitarian.world)*