ARCHIVED COPY

# Data Processing Agreement

**Version 1.0** | In force 15 November 2025 to 10 September 2026

Source: https://prduct.com/data-processing-agreement

Superseded by Schedule 2: Data Processing Agreement v2.0 (prduct.com/data-processing-agreement)

**SUPERSEDED 10 SEPTEMBER 2026: no longer applies to new acceptances**

*Last Updated: 15. November 2025*

## BACKGROUND AND SCOPE

**1.1 Purpose.** This Data Processing Agreement ("DPA") governs the processing of Personal Data by Prduct ApS ("Processor") on behalf of the Customer ("Controller") in connection with the Prduct Platform.

**1.2 Relationship to Terms.** This DPA is incorporated into and forms part of the Terms of Use and your Service Level Agreement (collectively, the "Agreement").

**1.3 Personal Data Processed.** The Platform processes limited Personal Data including:

- Contact information of sole proprietors and business contacts
- Names and email addresses of supplier/customer representatives
- User account information (names, emails, job titles)
- Communication logs between users

**1.4 Product Data is Not Personal Data.** The Platform's primary purpose is managing product data (specifications, compliance documentation, supply chain data). Such data relates to products, not individuals, and is not Personal Data under GDPR.

**1.5 Hierarchy.** If there is conflict: (1) Custom DPA (if negotiated) > (2) This DPA > (3) Agreement.

## 2. DEFINITIONS

**"Controller"** means the Customer who determines the purposes and means of processing Personal Data.

**"Data Subject"** means an identified or identifiable natural person whose Personal Data is processed.

**"GDPR"** means Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data.

**"Personal Data"** means any information relating to an identified or identifiable natural person, as defined in GDPR Article 4(1).

**"Processing"** means any operation performed on Personal Data, as defined in GDPR Article 4(2).

**"Processor"** means Prduct ApS.

**"Standard Contractual Clauses" or "SCCs"** means the EU Standard Contractual Clauses for international data transfers approved by the European Commission.

**“Sub-processor”** means any third party engaged by Processor to process Personal Data on behalf of Controller.

**“Supervisory Authority”** means an independent public authority established by an EU Member State pursuant to GDPR Article 51.

### 3. ROLES AND RESPONSIBILITIES

**3.1 Controller Obligations.** Controller is responsible for:

- Determining the legal basis for processing Personal Data
- Ensuring lawful collection and processing of Personal Data uploaded to the Platform
- Obtaining necessary consents from Data Subjects
- Providing privacy notices to Data Subjects
- Responding to Data Subject requests (Processor will assist per Section 8)
- Ensuring compliance with GDPR and applicable data protection laws

**3.2 Processor Obligations.** Processor will:

- Process Personal Data only on documented instructions from Controller
- Ensure personnel processing Personal Data are bound by confidentiality
- Implement appropriate technical and organizational security measures
- Assist Controller in responding to Data Subject requests
- Assist Controller with security incidents and data protection impact assessments
- Delete or return Personal Data upon termination (per Section 12)

**3.3 Instructions.** Processor processes Personal Data only on Controller’s documented instructions unless required by EU or Member State law. If Processor believes an instruction violates GDPR or applicable law, Processor will immediately inform Controller.

### 4. DETAILS OF PROCESSING

**4.1 Subject Matter:** Provision of the Prduct Platform (SaaS product data management and compliance platform).

**4.2 Duration:** For the term of the Agreement and during the wind-down period (30-90 days post-termination).

**4.3 Nature and Purpose:**

- Facilitating supply chain data exchange
- Managing product compliance documentation
- Enabling communication between supply chain partners
- Providing user account management
- Generating compliance reports and analytics

**4.4 Categories of Data Subjects:**

- Controller’s employees and contractors
- Sole proprietor suppliers/customers

- Contact persons at supplier/customer organizations
- Platform users within Controller's organization

**4.5 Types of Personal Data:**

- **Identification data:** Names, email addresses, phone numbers, job titles
- **Account data:** Login credentials (hashed), user preferences
- **Communication data:** Messages and chats between users
- **Business relationship data:** Company affiliations, roles in supply chain

**4.6 Sensitive Data.** The Platform is not designed to process Special Categories of Personal Data (GDPR Article 9) such as health data, biometric data, racial/ethnic origin, etc. Controller must not upload such data. If Controller uploads Sensitive Data in violation of this DPA, Controller is solely responsible.

**5. SECURITY MEASURES**

**5.1 Technical and Organizational Measures.** Processor implements appropriate security measures including:

**(a) Access Controls:**

- Two-factor authentication (2FA) available/required
- Role-based access control (RBAC)
- Unique user accounts (no shared credentials)
- Password complexity requirements (minimum 12 characters)
- Automatic session timeouts

**(b) Encryption:**

- Data in transit: TLS 1.2+ encryption
- Data at rest: AWS encryption for stored data
- Encrypted backups

**(c) Infrastructure Security:**

- AWS EU hosting (Stockholm/Frankfurt regions)
- Firewall protection
- Intrusion detection and prevention
- DDoS protection via AWS Shield
- Regular security patches and updates

**(d) Backup and Recovery:**

- Regular automated backups (frequency per tier)
- Geo-redundant backup storage (Premium/Enterprise)
- Tested recovery procedures

**(e) Monitoring and Logging:**

- Security event logging
- Access logging and audit trails

- Anomaly detection
- Regular log reviews

**(f) Physical Security:**

- AWS data center physical security (SOC 2 certified facilities)
- No on-premise servers maintained by Processor

**5.2 Security Documentation.** Detailed security measures available at prduct.com/security.

**5.3 ISO 27001 Alignment.** Processor's security controls are aligned with ISO 27001:2013/2022 standards. Formal certification is in progress (expected ultimo 2026).

**5.4 Security Testing.** Processor conducts:

- Regular vulnerability scanning
- Security code reviews

**5.5 Changes to Security Measures.** Processor may update security measures provided the overall level of security is not reduced. Material changes will be communicated to Controller.

**6. SUB-PROCESSORS**

**6.1 Authorization.** Controller authorizes Processor to engage Sub-processors listed at prduct.com/data-processing-agreement/sub-processors.

**6.2 Current Sub-processors:**

- **Amazon Web Services (AWS):** Cloud infrastructure and hosting (EU regions)
- **Intercom R&D Unlimited Company:** Support & sales
- **Microsoft Ireland Operations Limited:** Support and Sales, Cloud infrastructure and hosting of services and artificial intelligence.

**6.3 Sub-processor Obligations.** Processor ensures Sub-processors:

- Are bound by written agreements imposing substantially the same obligations as this DPA
- Implement appropriate security measures
- Process Personal Data only as instructed

**6.4 Notification of Changes.** Processor will notify Controller of any intended changes (addition/replacement of Sub-processors) via:

- Email to Controller's account email
- Update to prduct.com/data-processing-agreement/sub-processors
- Minimum 30 days' notice before new Sub-processor processes Personal Data

**6.5 Objection Right.** Controller may object to a new Sub-processor on reasonable grounds relating to data protection. Objection must be raised within 30 days of notification. If Controller objects:

- Parties will discuss alternative solutions in good faith
- If no solution is found, Controller may terminate the affected services with 30 days' notice (with pro-rata refund if applicable)

**6.6 Liability.** Processor remains fully liable to Controller for Sub-processor performance.

**7. INTERNATIONAL TRANSFERS**

**7.1 Data Location.** Personal Data is primarily processed and stored in the EU (AWS Stockholm/Frankfurt regions).

**7.2 Sub-processors Outside EU.** Some Sub-processors may process Personal Data outside the EU/EEA. For such transfers:

- **Standard Contractual Clauses:** EU SCCs (Module 2: Controller-to-Processor) apply automatically
- **Additional Safeguards:** Processor implements supplementary technical measures (encryption, access controls)
- **Assessment:** Processor conducts transfer impact assessments

**7.3 SCC Incorporation.** The EU Standard Contractual Clauses (Decision 2021/914) are incorporated by reference and form Appendix 1 to this DPA, with:

- **Module 2** (Controller-to-Processor) applies
- **Annex I:** Details in Section 4 of this DPA
- **Annex II:** Security measures in Section 5 of this DPA
- **Annex III:** Sub-processors in Section 6 of this DPA
- **Governing Law:** Clause 17: Danish law
- **Jurisdiction:** Clause 18: Danish courts (Aarhus)

**7.4 UK Transfers.** For transfers to/from the UK: UK International Data Transfer Agreement or UK Addendum to EU SCCs applies.

**7.5 Adequacy Decisions.** If the EU Commission adopts an adequacy decision for a relevant third country, transfers to that country may rely on such decision.

**8. DATA SUBJECT RIGHTS**

**8.1 Controller Responsibility.** Controller is responsible for responding to Data Subject requests (access, rectification, erasure, restriction, portability, objection).

**8.2 Processor Assistance.** Upon Controller’s request, Processor will provide reasonable assistance to enable Controller to respond to Data Subject requests, including:

- Providing relevant Personal Data in Processor’s possession
- Technical means to export Personal Data
- Guidance on Platform functionality for data retrieval

**8.3 Direct Requests.** If Processor receives a Data Subject request directly, Processor will:

- Forward the request to Controller without undue delay (within 48 hours)
- Not respond to the Data Subject without Controller’s prior authorization (unless legally required)

**8.4 Fees.** Assistance beyond basic cooperation may be subject to reasonable fees based on time and complexity.

**9. DATA BREACH NOTIFICATION**

**9.1 Notification Obligation.** Processor will notify Controller without undue delay (target: within 48 hours) after becoming aware of a Personal Data breach affecting Controller's Personal Data.

**9.2 Breach Notification Content:**

- Nature of the breach (categories and approximate number of Data Subjects affected)
- Contact point for more information (security@prduct.com)
- Likely consequences of the breach
- Measures taken or proposed to address the breach and mitigate effects

**9.3 Staged Notification.** If full information is not immediately available, Processor will provide information in phases without undue delay.

**9.4 Documentation.** Processor will document all Personal Data breaches, including facts, effects, and remedial actions. Documentation available to Controller and Supervisory Authorities upon request.

**9.5 Controller's Responsibility.** Controller is responsible for determining whether to notify Data Subjects and Supervisory Authorities per GDPR Articles 33-34.

**10. DATA PROTECTION IMPACT ASSESSMENT (DPIA)**

**10.1 Assistance.** If Controller is required to conduct a DPIA under GDPR Article 35, Processor will provide reasonable assistance, including:

- Information about Processing operations
- Security measures implemented
- Information about Sub-processors
- Information about data flows

**10.2 Prior Consultation.** If Controller must consult a Supervisory Authority under GDPR Article 36, Processor will provide necessary information and assistance.

**10.3 Fees.** Extensive DPIA assistance beyond basic cooperation may be subject to reasonable fees.

**11. AUDITS AND INSPECTIONS**

**11.1 Audit Rights.** Controller may audit Processor's compliance with this DPA, subject to:

- Reasonable advance notice (minimum 30 days)
- Maximum frequency: once per year (unless breach or regulatory requirement)
- Conducted during business hours
- Reasonable scope and duration
- Controller's expense
- Confidentiality obligations

**11.2 Third-Party Audits.** Controller may appoint independent third-party auditor (subject to Processor's approval, not to be unreasonably withheld).

**11.3 Certifications and Reports.** As an alternative to audits, Processor may provide:

- ISO 27001 certificates (when available)
- SOC 2 reports (when available)

- Third-party security assessments

**11.4 Audit Costs.** Controller bears all audit costs. If audit reveals material non-compliance, Processor bears reasonable audit costs.

**11.5 Sub-processor Audits.** For Sub-processor audits, Processor will obtain and provide relevant audit reports/certifications where available (e.g., AWS SOC 2 reports).

**12. DATA DELETION AND RETURN**

**12.1 Upon Termination.** Within 30 days after termination of the Agreement, Processor will (at Controller's choice):

- Delete all Personal Data and existing copies; OR
- Return all Personal Data to Controller in a standard machine-readable format (CSV/JSON)

**12.2 Grace Period for Retrieval.** Controller has 30 days from termination to request data export. After 30 days, data may be deleted without further notice.

**12.3 Deletion Certification.** Upon request, Processor will provide written certification that Personal Data has been deleted.

**12.4 Legal Retention.** Processor may retain Personal Data to the extent required by EU or Member State law (e.g., accounting records, legal claims). Such retained data remains subject to confidentiality and security obligations.

**12.5 Backup Deletion.** Personal Data in backups will be deleted per Processor's standard backup retention schedules (maximum 365 days for Enterprise tier).

**12.6 Anonymized Data Retention.** Processor may retain anonymized/aggregated data that cannot be linked to Controller or Data Subjects, as specified in the Agreement (Terms of Use Section 8.2).

**13. CONFIDENTIALITY**

**13.1 Personnel.** Processor ensures all personnel authorized to process Personal Data:

- Are bound by confidentiality obligations (contractual or statutory)
- Receive appropriate training on data protection
- Have access only on a need-to-know basis

**13.2 Survival.** Confidentiality obligations survive termination of this DPA indefinitely.

**14. LIABILITY AND INDEMNIFICATION**

**14.1 GDPR Liability.** Each party's liability under GDPR Articles 82-83 is governed by those provisions.

**14.2 Contractual Liability.** Subject to Section 14.1, liability is governed by the Agreement (Terms of Use Section 11).

**14.3 Indemnification.** Each party will indemnify the other against third-party claims arising from:

- The indemnifying party's breach of this DPA
- The indemnifying party's violation of GDPR
- The indemnifying party's negligence or willful misconduct

Indemnification is subject to: (a) prompt notice of claim; (b) reasonable cooperation; (c) sole control of defense.

**15. TERM AND TERMINATION**

**15.1 Term.** This DPA commences on the Effective Date and continues for the term of the Agreement.

**15.2 Survival.** Sections 5 (Security), 9 (Breach), 12 (Deletion), 13 (Confidentiality), and 14 (Liability) survive termination.

**15.3 Termination for Breach.** Either party may terminate this DPA if the other party:

- Commits a material breach and fails to cure within 14 days of written notice
- Violates GDPR in a manner that creates risk of significant harm to Data Subjects
- Fails to comply with a binding decision of a Supervisory Authority

**15.4 Effect of DPA Termination.** If this DPA terminates, Processor will immediately cease processing Personal Data (except as required for data return/deletion per Section 12).

**16. MODIFICATIONS**

**16.1 Changes.** Processor may modify this DPA to:

- Comply with changes in GDPR or other data protection laws
- Reflect new Standard Contractual Clauses approved by the EU Commission
- Address guidance from Supervisory Authorities

**16.2 Notice.** Material changes will be notified 30 days in advance via email and posting at prduct.com/dpa.

**16.3 Objection.** If Controller objects to material changes, Controller may terminate the Agreement per Terms of Use Section 14.4.

**17. GENERAL PROVISIONS**

**17.1 Entire Agreement.** This DPA, together with the Agreement, constitutes the entire agreement regarding data processing.

**17.2 Conflict.** In case of conflict between this DPA and the Agreement, this DPA prevails on data protection matters.

**17.3 Severability.** If any provision is found invalid, the rest remains in effect. Parties will negotiate a valid replacement provision.

**17.4 No Waiver.** Failure to enforce any provision is not a waiver.

**17.5 Third-Party Rights.** No third-party beneficiaries except as required by SCCs.

**18. GOVERNING LAW AND JURISDICTION**

**18.1 Governing Law.** This DPA is governed by Danish law.

**18.2 Jurisdiction.** Disputes will be resolved in Danish courts (Aarhus), except:

- Data Subjects may bring claims in their EU Member State of residence per GDPR Article 79
- Supervisory Authorities have jurisdiction per GDPR Article 56

**18.3 SCC Governance.** For matters governed by the incorporated Standard Contractual Clauses, the SCCs' governing law and jurisdiction provisions apply.

## 19. CONTACT INFORMATION

**For Data Protection Matters:**
Prduct ApS
Data Protection Officer: dpo@prduct.com
Address: Universitetsbyen 71, 8000 Aarhus C, Denmark
Phone: +45 5020 8844

**For Security Incidents:**
security@prduct.com

**For General Inquiries:**
legal@prduct.com

## 20. ACCEPTANCE

By accepting the Terms of Use or signing an Order Form that references this DPA, Controller accepts this Data Processing Agreement.