PRDUCT APS | LEGAL

Schedule 2: Data Processing Agreement

Version 2.0 | Effective 10 September 2026 | https://prduct.com/data-processing-agreement
Replaces the Data Processing Agreement (15 November 2025).

Prduct ApS
Last Updated: 10 September 2026

1. BACKGROUND AND SCOPE

1.1 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 This DPA forms Schedule 2 to the Subscription Agreement and is incorporated into the Terms of Use (each an "Agreement"). It applies to every Controller whose Customer Data contains Personal Data, whether or not the Controller has a Subscription Agreement.

1.3 The Platform processes limited Personal Data: 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 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.

1.5 Hierarchy: (1) a custom DPA signed by both parties; (2) this DPA; (3) the Agreement.

2. DEFINITIONS

"Controller", "Data Subject", "Personal Data", "Processing" and "Supervisory Authority" have the meanings given in the GDPR (Regulation (EU) 2016/679). "Processor" means Prduct ApS. "Sub-processor" means a third party engaged by Processor to process Personal Data on behalf of Controller. "SCCs" means the EU Standard Contractual Clauses for international transfers (Decision 2021/914).

“Connected Controller” means another Controller with whom the Controller exchanges Shared Data through the Platform under Terms of Use Section 15.

3. ROLES AND INSTRUCTIONS

3.1 Controller is responsible for the lawfulness of the Personal Data uploaded to the Platform, for the legal basis, for notices to Data Subjects, and for responding to Data Subject requests (with Processor's assistance under Section 8).

3.2 Processor will process Personal Data only on documented instructions, bind its personnel to confidentiality, implement appropriate security measures, assist Controller under Sections 8 to 10, and delete or return Personal Data under Section 12.

3.3 Documented instructions. Controller instructs Processor to process Personal Data: (a) to provide, maintain and secure the Platform in accordance with the Agreement; (b) to make Shared Data visible to Connected Controllers in accordance with Controller's sharing settings; and (c) to derive anonymised and aggregated data from Customer Data in such a way that the resulting data can no longer be related to an

identified or identifiable natural person, a specific Controller, brand or product. Data anonymised under (c) is no longer Personal Data and falls outside this DPA. Processor applies anonymisation techniques consistent with guidance from the European Data Protection Board and the Danish Data Protection Agency.

3.4 If Processor considers that an instruction infringes the GDPR or other applicable law, Processor will inform Controller without delay. Processing required by EU or Member State law is permitted; Processor will inform Controller of the requirement unless the law prohibits it.

3.5 Connected Controllers. Where Personal Data is exchanged between Controller and a Connected Controller through the Platform, each acts as an independent controller of that Personal Data for its own purposes, and Processor acts as processor for each of them under this DPA. Controller and the Connected Controller are not joint controllers.

4. DETAILS OF PROCESSING

4.1 Subject matter: provision of the Prduct Platform (SaaS product data management and compliance platform).

4.2 Duration: the term of the Agreement and the wind-down period under Section 12.

4.3 Nature and purpose: facilitating supply chain data exchange; managing product compliance documentation; enabling communication between supply chain partners; user account management; compliance reports and analytics.

4.4 Categories of Data Subjects: Controller's employees and contractors; sole proprietor suppliers/customers; contact persons at supplier/customer organisations; Platform users within Controller's organisation.

4.5 Types of Personal Data: identification data (names, email addresses, phone numbers, job titles); account data (hashed credentials, preferences); communication data (messages between users); business relationship data (company affiliations, roles in supply chain).

4.6 The Platform is not designed to process special categories of Personal Data (GDPR Article 9). Controller must not upload such data and is solely responsible if it does.

5. SECURITY MEASURES

5.1 Processor implements appropriate technical and organisational measures, including: access controls (single sign-on through Microsoft Entra ID using OpenID Connect, two-factor authentication, role-based access, unique accounts, password requirements, session timeouts); encryption in transit (TLS 1.2+) and at rest (AWS encryption, encrypted backups); malicious code protection (scanning of uploaded files and email attachments for malware through AWS GuardDuty before they are made available in the Platform); infrastructure security (AWS EU hosting in Stockholm/Frankfurt, firewalls, intrusion detection, DDoS protection); backup and recovery (automated backups, geo-redundancy for Premium/Enterprise, tested recovery); monitoring and logging (AWS GuardDuty threat detection, security event logging, audit trails, anomaly detection); physical security through AWS data centres.

5.2 Detailed security measures and current certification status are published at prduct.com/security.

5.3 Processor's security controls are aligned with ISO 27001. Certification status is published at prduct.com/security.

5.4 Processor conducts regular vulnerability scanning and security code reviews.

5.5 Processor may update security measures provided the overall level of security is not reduced. Material changes are communicated to Controller.

6. SUB-PROCESSORS

6.1 Controller authorises Processor to engage the Sub-processors listed at prduct.com/data-processing-agreement/sub-processors.

6.2 Current Sub-processors: Amazon Web Services (cloud infrastructure and hosting, EU regions); Intercom R&D Unlimited Company (support and sales); Microsoft Ireland Operations Limited (support and sales, cloud infrastructure and hosting, artificial intelligence services).

6.3 Processor ensures Sub-processors are bound by written agreements imposing substantially the same obligations as this DPA, implement appropriate security measures, and process Personal Data only as instructed.

6.4 Processor notifies Controller of intended changes of Sub-processors by email to Controller's account email and by updating the list, at least 30 days before the new Sub-processor processes Personal Data.

6.5 Controller may object on reasonable data protection grounds within 30 days of notification. The parties will discuss alternatives in good faith; if none is found, Controller may terminate the affected services with 30 days' notice and a pro-rata refund where applicable.

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

7. INTERNATIONAL TRANSFERS

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

7.2 Where a Sub-processor processes Personal Data outside the EU/EEA, the EU SCCs (Module 2, Controller-to-Processor) apply, supplemented by technical measures (encryption, access controls) and a transfer impact assessment.

7.3 The SCCs (Decision 2021/914) are incorporated by reference as Appendix 1: Module 2 applies; Annex I is Section 4; Annex II is Section 5; Annex III is Section 6; governing law (Clause 17) Danish law; forum (Clause 18) Danish courts, Aarhus.

7.4 For transfers to or from the UK, the UK International Data Transfer Agreement or the UK Addendum to the EU SCCs applies.

7.5 Where an EU adequacy decision covers a third country, transfers may rely on that decision.

8. DATA SUBJECT RIGHTS

8.1 Controller is responsible for responding to Data Subject requests.

8.2 On request, Processor provides reasonable assistance, including relevant Personal Data in its possession, technical means to export Personal Data, and guidance on Platform functionality.

8.3 If Processor receives a request directly, it forwards the request to Controller within 48 hours and does not respond to the Data Subject without Controller's authorisation unless legally required.

8.4 Assistance beyond basic cooperation may be subject to reasonable fees.

9. PERSONAL DATA BREACH

9.1 Processor notifies Controller without undue delay, and targets notification within 48 hours, after becoming aware of a Personal Data breach affecting Controller's Personal Data.

9.2 The notification describes the nature of the breach (categories and approximate number of Data Subjects), a contact point (security@prduct.com), likely consequences, and measures taken or proposed. Information may be provided in phases.

9.3 Processor documents all Personal Data breaches. Documentation is available to Controller and Supervisory Authorities on request.

9.4 Controller determines whether to notify Data Subjects and Supervisory Authorities under GDPR Articles 33 and 34.

10. DATA PROTECTION IMPACT ASSESSMENT

10.1 Processor provides reasonable assistance with DPIAs (GDPR Article 35) and prior consultations (Article 36), including information on processing operations, security measures, Sub-processors and data flows. Extensive assistance may be subject to reasonable fees.

11. AUDITS

11.1 Controller may audit Processor's compliance with this DPA once per year (more often after a breach or on regulatory requirement), with at least 30 days' notice, during business hours, at Controller's expense, within a reasonable scope and subject to confidentiality.

11.2 Controller may appoint an independent third-party auditor, subject to Processor's approval, not to be unreasonably withheld.

11.3 As an alternative, Processor may provide ISO 27001 certificates, SOC 2 reports or third-party security assessments where available, and relevant Sub-processor audit reports (e.g. AWS SOC 2).

11.4 If an audit reveals material non-compliance, Processor bears the reasonable audit costs.

12. DELETION AND RETURN

12.1 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 in a standard machine-readable format (CSV/JSON).

12.2 Controller has 30 days from termination to request export. Thereafter data may be deleted without further notice.

12.3 On request, Processor certifies deletion in writing.

12.4 Processor may retain Personal Data to the extent required by EU or Member State law, subject to continuing confidentiality and security obligations.

12.5 Personal Data in backups is deleted per Processor's backup retention schedule (maximum 365 days for Enterprise).

12.6 Processor may retain anonymised and aggregated data that cannot be linked to Controller or Data Subjects, as instructed in Section 3.3(c) and provided in Terms of Use Section 8.2.

13. CONFIDENTIALITY

13.1 Processor ensures that all personnel authorised to process Personal Data are bound by confidentiality, receive appropriate training, and have access only on a need-to-know basis.

13.2 Confidentiality obligations survive termination indefinitely.

14. LIABILITY

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

14.2 Subject to Section 14.1, contractual liability is governed by Terms of Use Section 11 or, for Controllers with a Subscription Agreement, Section 10 of that agreement.

14.3 Each party indemnifies the other against third-party claims arising from the indemnifying party's breach of this DPA, violation of the GDPR, or negligence or wilful misconduct, subject to prompt notice, reasonable cooperation and sole control of the defence.

15. TERM

15.1 This DPA applies for the term of the Agreement. Sections 5, 9, 12, 13 and 14 survive termination.

15.2 Either party may terminate this DPA if the other commits a material breach not cured within 14 days of written notice, violates the GDPR in a manner that creates a risk of significant harm to Data Subjects, or fails to comply with a binding decision of a Supervisory Authority. On termination Processor ceases processing except for return or deletion under Section 12.

16. CHANGES

16.1 Processor may amend this DPA to comply with changes in data protection law, to reflect new SCCs, or to address Supervisory Authority guidance. Material changes are notified 30 days in advance by email and at prduct.com/data-processing-agreement.

16.2 If Controller objects to a material change, Terms of Use Section 17 or Subscription Agreement Section 12 applies.

17. GENERAL

17.1 This DPA prevails over the Agreement in matters concerning the processing of Personal Data.

17.2 If any provision is invalid, the rest remains in effect and the parties will negotiate a valid replacement. Failure to enforce a provision is not a waiver. There are no third-party beneficiaries except as required by the SCCs.

18. GOVERNING LAW AND JURISDICTION

18.1 This DPA is governed by Danish law. Disputes are resolved by the Danish courts (Aarhus), except that Data Subjects may bring claims under GDPR Article 79 and Supervisory Authorities have competence under Article 56. For matters governed by the SCCs, the SCCs' provisions apply.

19. CONTACT

Prduct ApS, Universitetsbyen 71, 8000 Aarhus C, Denmark
Data Protection Officer: dpo@prduct.com
Security incidents: security@prduct.com
General: legal@prduct.com

20. ACCEPTANCE

Controller accepts this DPA by accepting the Terms of Use or the Subscription Agreement, each of which incorporates it.