Jaws Deploy AS Data Processing Agreement
Addendum to Service Agreement
Effective Date: 1 October 2025

This Data Processing Agreement ("DPA") is an addendum to the Jaws Deploy AS Service Agreement ("Service Agreement") between you and Jaws Deploy AS, a Norwegian company with organization number 933 925 935, located at Grenseveien 10, 1406 Ski, Norway ("Jaws Deploy", "we", "us", or "our"). It applies when we process Your Personal Information as a Processor on your behalf as a Controller, as defined under Applicable Data Protection Laws, in connection with our Services, which include On-Premise software and Cloud-based solutions, including Jaws Deploy Cloud.

We enter this DPA on behalf of ourselves and our Affiliates. If your Affiliates use our Services or provide Your Personal Information under the Service Agreement, you enter this DPA on their behalf. References to "we," "us," or "our" include our Affiliates, and "you" or "your" include your Affiliates, solely for this DPA's purposes, without imposing additional rights or obligations under the Service Agreement.

In case of conflict between this DPA and the Service Agreement, this DPA prevails for privacy and data security matters, while the Service Agreement governs all other matters.

1. Terms and Definitions

1.1 Key Definitions

- **Affiliate**: An entity controlling, controlled by, or under common control with a party, with control meaning over 50% ownership of voting interests.
- **Applicable Data Protection Laws**: The Norwegian Personal Data Act (Personopplysningsloven), GDPR, and any other laws governing Your Personal Information to which we or our Subprocessors are subject.
- **Controller**: You, as the entity determining the purposes and means of processing Your Personal Information under Applicable Data Protection Laws.
- **Data Subject**: An individual to whom Your Personal Information relates.
- **GDPR**: EU General Data Protection Regulation 2016/679.
- **Personal Data Breach**: Unauthorized or unlawful processing, disclosure, access, loss, alteration, or destruction of Your Personal Information.
- **Processor**: Jaws Deploy, processing Your Personal Information on your behalf as Controller.
- **Standard Contractual Clauses (SCCs)**: Module 2 (Controller to Processor) clauses approved by the European Commission under Commission Decision 2021/914, as amended.
- **Subprocessor**: A third party we appoint to process Your Personal Information on your behalf under this DPA, excluding our employees or agents.

- **Your Personal Information**: Information within Your Information (as defined in the Service Agreement) relating to an identified or identifiable individual, as defined under Applicable Data Protection Laws.

1.2 Interpretation

"Includes" is non-limiting. Singular and plural terms are interchangeable. This DPA is not construed against its drafter.

2. Processing Obligations

2.1 Purpose and Compliance

We will process Your Personal Information only to provide our Services under the Service Agreement and this DPA, in compliance with Applicable Data Protection Laws, including the Norwegian Personal Data Act and GDPR.

2.2 Your Instructions

We will process Your Personal Information based on your written instructions, including authorizations in the Service Agreement. If required to process Your Personal Information to comply with Applicable Data Protection Laws, we will notify you beforehand unless prohibited by law on public interest grounds.

3. Confidentiality and Security Measures

3.1 Access Restrictions

We will restrict access to Your Personal Information to our employees, agents, Affiliates, and Subprocessors who need access to fulfill the Service Agreement and this DPA, subject to confidentiality obligations (contractual or legal).

3.2 Security Standards

We will implement technical and organizational measures to ensure a security level appropriate to the risk, including, as applicable:

(a) pseudonymization and encryption of Your Personal Information;

(b) measures to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems;

(c) ability to restore access to Your Personal Information promptly after an incident;

(d) regular testing and evaluation of security measures' effectiveness.

These measures will consider:

(a) technological advancements;

(b) implementation costs;

(c) processing nature, scope, context, and purposes;

(d) risks to Data Subjects' rights and freedoms, including from a Personal DataBreach.

3.3 Security Implementation

Our minimum security measures include:

- **Encryption**: Strong encryption for Your Personal Information in transit over public networks.
- **Storage**: Secure physical and logical environments to prevent unauthorized access, modification, or loss.
- **Firewalls**: Restricting network traffic to necessary ports and services, blocking all others.
- **Endpoint Protection**: Tools to detect and prevent malicious software.
- **Vulnerability Management**: Timely application of critical patches (within 30 days for zero-day vulnerabilities) using a risk-based approach.
- **Audit Logging**: Daily review of logs for privileged access, unauthorized attempts, and security events, with restricted access to logs.
- **Data Loss Prevention**: Controls to prevent unauthorized data loss, integrated with intrusion detection systems.
- **Physical Security**: Secure facilities with environmental and access controls.

4. Subprocessor Engagement

4.1 Subprocessor Use

We may engage Subprocessors, with a current list published at www.jawsdeploy.net. We will update this list before engaging or changing Subprocessors, providing notice via the website. You may object within 14 days; if unresolved, you may terminate the affected Services per the Service Agreement.

4.2 Subprocessor Obligations

We will ensure Subprocessors are bound by written agreements requiring equivalent data protection standards as this DPA, including compliance with Applicable Data Protection Laws.

4.3 Subprocessor Liability

We remain liable for any Subprocessor's breach of this DPA.

5. Personal Data Breach Response

5.1 Notification

We will notify you of a Personal Data Breach without undue delay after becoming aware, providing details on the breach's nature, likely consequences, and our mitigation measures.

5.2 Cooperation

We will assist you with reasonable steps to investigate, mitigate, and remediate a Personal Data Breach. If your requested assistance exceeds legal requirements, we may request reimbursement of reasonable costs, where permitted by Applicable Data Protection Laws.

6. Data Subject Rights

6.1 Request Notification

We will promptly notify you if we receive a request, notice, or complaint from a Data Subject regarding Your Personal Information, where you are the Controller and we are the Processor.

6.2 Cooperation

We will provide reasonable assistance to help you respond to Data Subject requests and comply with Applicable Data Protection Laws, including enabling you to manage Your Personal Information.

7. Post-Termination Data Handling

7.1 Deletion or Return

Upon termination or expiry of the Service Agreement, we will delete or return Your Personal Information as required by Applicable Data Protection Laws and the Service Agreement, unless retention is permitted or required by law.

7.2 Retention

Any retained Personal Information will remain confidential and be processed only as permitted by Applicable Data Protection Laws.

8. Assistance with Compliance

8.1 Data Protection Assessments

We will provide reasonable assistance for data protection impact assessments or consultations with data protection authorities (e.g., Datatilsynet in Norway) regarding our or our Subprocessors' processing of Your Personal Information.

8.2 Cost Reimbursement

Where permitted by Applicable Data Protection Laws, we may request reimbursement for reasonable costs of assistance exceeding legal requirements.

9. Audit and Compliance

9.1 Information Requests

We will provide information reasonably necessary to demonstrate compliance with this DPA, including relevant records or audits, subject to this section.

9.2 Request Limits

Youmayrequestcomplianceinformationoncepercalendaryearunlessrequired by Applicable Data Protection Laws or justified by genuine concerns, with reasons provided.

9.3 Scope of Requests

Requests are limited to information relevant to our compliance with Applicable Data Protection Laws, not general business information.

9.4 Confidentiality of Information

Persons receiving compliance information must keep it confidential, except as needed to confirm our compliance, and return or destroy it upon delivering their report to you, at our discretion.

9.5 Response Time

We require reasonable time to respond to requests, typically 30 days.

9.6 Audit Conditions

If audits involve our infrastructure or premises, your representatives must minimize disruption and comply with our security policies. We may require evidence of their identity or authority.

9.7 Cost Reimbursement

We may request reimbursement for reasonable costs of assistance exceeding legal requirements, where permitted by Applicable Data Protection Laws.

10. Cross-Border Data Transfers

10.1 GDPR Transfers

If we process Your Personal Information from the EU/EEA under GDPR, and the transfer is to a country without an adequacy decision from the European Commission, it constitutes an "EU SCC Transfer." We will comply with Module 2 SCCs, with:

(a) Clause 7 (docking) excluded;

(b) Clause9, Option2(generalauthorization)applied, withSubprocessorchangesnotified per Section 4.1;

(c) Clause 11(a) "OPTION" excluded, with bracketed wording deleted.

10.2 Alternative Measures

If SCCs do not provide adequate protection, we will collaborate with you to implement alternative measures to ensure compliance with Applicable Data Protection Laws.

10.3 Consent to Transfers

Subject to compliance with this section, you consent to our transferring Your Personal Information outside the EU/EEA.

11. General Provisions

11.1 Conflict Resolution

If this DPA conflicts with the SCCs, the SCCs prevail to the extent of the inconsistency.

11.2 Governing Law

This DPA is governed by Norwegian law, including the Norwegian Personal Data Act, with disputes subject to the exclusive jurisdiction of Oslo District Court (Oslo Tingrett), as per the Service Agreement.

11.3 Severability

Invalid provisions are severed, and the remaining DPA remains enforceable.

11.4 Survival

Sections 2, 3, 4, 5, 6, 7, 8, and 9 survive termination of the Service Agreement.

11.5 Notices

Notices must be in writing and sent to admin@jawsdeploy.net (our address for notices) or to your registered contact details. Notices are effective upon confirmed delivery.

Schedule 1: Data Processing Particulars

Details of processing (e.g., categories of Your Personal Information, Data Subjects, purposes) will be specified in the Service Agreement or order documentation, including types of data processed for Jaws Deploy Cloud and On-Premise
Services.

Schedule 2: Technical and Organizational Security Measures

Our security measures, as described in Section 3.2, include but are not limited to:

1. Encryption of Your Personal Information in transit and at rest.
2. Secure storage environments to prevent unauthorized access or loss.
3. Firewalls restricting unnecessary network traffic.

4. Endpoint protection against malicious software.
5. Vulnerability management with timely critical patch application.
6. Daily audit log reviews and intrusion detection systems.
7. Data loss prevention controls.
8. Physical security of facilities.

We may update these measures to reflect technological advancements, maintaining or enhancing security levels.