RelineAI

Data Processing Agreement

(DPA)

Addendum to the Application Terms and Conditions

Effective Date: 31.03.2026

RelineAI Sp. z o.o.
ul. Ignacego Mościckiego 1, 24-110 Puławy, Poland
KRS: 0001174513 | NIP: 7162848161 | REGON: 541791712
Contact: contact@relineai.com | Privacy: privacy@relineai.com

Table of Contents

1. Introduction and Scope

1.1 This Data Processing Agreement ("**DPA**") forms an integral part of, and is supplementary to, the Application Terms and Conditions ("**Agreement**") between RelineAI Sp. z o.o. ("**Processor**", "**RelineAI**") and any Client or User ("**Controller**") who processes personal data through the RelineAI Application.

1.2 This DPA applies automatically to all Users and Clients who process personal data through the RelineAI Application. By using the Application, the Controller agrees to the terms of this DPA.

1.3 This DPA is designed as a self-service, website-publishable document and does not require individual signatures. Acceptance occurs through the use of the Application, as stipulated in the Agreement.

1.4 In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to the processing of personal data.

2. Definitions

For the purposes of this DPA, the following terms shall have the meanings set out below. Capitalized terms not defined herein shall have the meanings given to them in the Agreement or in the GDPR.

"Controller" means the Client or User who determines the purposes and means of the processing of Personal Data and who uses the RelineAI Application under the Agreement.

"Processor" means RelineAI Sp. z o.o., which processes Personal Data on behalf of the Controller in connection with the provision of the Application.

"Personal Data" means any personal data, as defined in Article 4(1) of the GDPR, processed by the Processor on behalf of the Controller through the Application.

"Sub-processor" means any third party engaged by the Processor to process Personal Data on behalf of the Controller.

"Processing" means any operation or set of operations performed on Personal Data, as defined in Article 4(2) of the GDPR, including but not limited to collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, or destruction.

"Data Protection Laws" means the General Data Protection Regulation (EU) 2016/679 ("GDPR"), and any applicable national implementing legislation of the EU Member States, as well as any other applicable data protection or privacy laws.

"Data Subject" means an identified or identifiable natural person whose Personal Data is processed under this DPA.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed, as defined in Article 4(12) of the GDPR.

"Application" means the RelineAI software-as-a-service platform for retail store layout generation, as described in the Agreement.

3. Roles and Responsibilities

3.1 The Controller acts as the data controller within the meaning of Article 4(7) of the GDPR, determining the purposes and means of the processing of Personal Data within the Application.

3.2 RelineAI acts as the data processor within the meaning of Article 4(8) of the GDPR, processing Personal Data solely on behalf of the Controller and in accordance with the Controller's documented instructions.

3.3 The Processor shall process Personal Data only to the extent necessary for the provision of the Application services as described in the Agreement and in accordance with the Controller's documented instructions, unless required to do so by European Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such notification on important grounds of public interest.

4. Subject Matter and Details of Processing

The following table describes the subject matter, nature, purpose, and scope of the processing carried out by the Processor on behalf of the Controller:

Subject Matter	Provision of the RelineAI retail layout generation platform as a software-as-a-service solution.
Duration of Processing	For the term of the Agreement between the Controller and the Processor, plus any applicable data retention period as specified in Section 11 of this DPA.
Nature of Processing	Storage, organization, structuring, retrieval, consultation, display, and export of data within the Application. Automated processing for layout generation using evolutionary algorithms.
Purpose of Processing	Enabling the Controller to use the Application for retail store layout generation, project management, collaboration, and related services as described in the Agreement.
Types of Personal Data	User account data (full name, email address, role/position within the Controller's organization), project metadata (creator, contributors, modification history), activity and audit logs (user actions, timestamps, IP addresses).
Categories of Data Subjects	Controller's employees, contractors, consultants, and other authorized users who access the Application on behalf of the Controller.

5. Obligations of the Processor

In accordance with Article 28(3) of the GDPR, the Processor shall:

(a) Process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(b) Ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) Implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as described in Annex 1 to this DPA, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

(d) Respect the conditions referred to in Section 6 of this DPA for engaging Sub-processors, including obtaining the Controller's prior general authorization before engaging any Sub-processor and imposing the same data protection obligations on the Sub-processor by way of a written agreement.

(e) Taking into account the nature of the processing, assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR.

(f) Assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the Processor.

(g) At the choice of the Controller, delete or return all the Personal Data to the Controller after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data. The Controller shall have a 30-day export window following the termination of the Agreement, as further described in Section 11.

(h) Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, subject to the conditions set out in Section 12 of this DPA.

5.2 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

6. Sub-Processors

6.1 The Controller grants the Processor a general written authorization to engage Sub-processors for the performance of specific processing activities on behalf of the Controller, in accordance with Article 28(2) of the GDPR.

6.2 The current list of Sub-processors engaged by the Processor is set out in Annex 2 to this DPA. The Controller acknowledges and approves the Sub-processors listed in Annex 2 as of the effective date of this DPA.

6.3 The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors. Such notification shall be provided via email to the Controller's registered email address or by publication on the RelineAI website, giving the Controller the opportunity to object to such changes.

6.4 The Controller may object to a new Sub-processor by notifying the Processor in writing within thirty (30) calendar days of receiving notice of the change. The objection must be based on reasonable grounds relating to data protection. If the Controller objects, the parties shall discuss the objection in good faith with a view to achieving a commercially reasonable resolution. If no resolution can be reached within thirty (30) days of the Processor's receipt of the objection, the Controller may terminate the Agreement upon written notice, without penalty.

6.5 Where the Processor engages a Sub-processor, the Processor shall impose on the Sub-processor, by way of a written agreement, the same data protection obligations as set out in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing meets the requirements of the GDPR.

6.6 The Processor shall remain fully liable to the Controller for the performance of the Sub-processor's obligations under its agreement with the Processor.

7. International Data Transfers

7.1 The Processor primarily processes Personal Data within the European Economic Area (EEA). The Application infrastructure is hosted on Microsoft Azure in EU regions, specifically Ireland and the Netherlands.

7.2 The Processor shall not transfer Personal Data to a country outside the EEA or to an international organization unless one of the following conditions is met:

- The European Commission has decided that the third country, a territory, or one or more specified sectors within that third country, or the international organization in question, ensures an adequate level of protection (Article 45 GDPR).
- Appropriate safeguards have been provided pursuant to Article 46 of the GDPR, including but not limited to Standard Contractual Clauses (SCCs) adopted by the European Commission.
- A derogation for specific situations under Article 49 of the GDPR applies.

7.3 As of the effective date of this DPA, Microsoft Azure, the primary infrastructure provider, operates under the EU-US Data Privacy Framework for any incidental transfers to the United States. Microsoft has obtained certification under the EU-US Data Privacy Framework and is committed to comply with the EU-US DPF Principles with regard to all personal data received from the EU.

7.4 Where required, the Processor shall enter into Standard Contractual Clauses (SCCs) as adopted by the European Commission with any Sub-processor located outside the EEA, supplemented by additional safeguards where necessary based on a transfer impact assessment.

8. Security Measures

8.1 The Processor shall implement and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, or disclosure. The specific measures in place as of the effective date of this DPA are described in Annex 1.

8.2 The Processor shall regularly review and update the security measures to ensure their continued appropriateness, taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing, and the risks to the rights and freedoms of Data Subjects.

8.3 The Processor shall notify the Controller of any material changes to the technical and organizational measures that may adversely affect the security of Personal Data.

9. Data Breach Notification

9.1 The Processor shall notify the Controller without undue delay, and in any event within twenty-four (24) hours after becoming aware of a Personal Data Breach affecting the Controller's Personal Data.

9.2 The notification shall include, to the extent available:

(a) A description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned.

(b) The name and contact details of the Processor's data protection officer or other contact point where more information can be obtained.

(c) A description of the likely consequences of the Personal Data Breach.

(d) A description of the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.3 Where it is not possible to provide all information at the same time, the information may be provided in phases without undue further delay.

9.4 The Processor shall assist the Controller in meeting the Controller's obligations under Articles 33 and 34 of the GDPR, taking into account the nature of processing and the information available to the Processor.

9.5 The Processor shall document any Personal Data Breach, comprising the facts relating to the breach, its effects, and the remedial action taken, and make this documentation available to the Controller upon request.

10. Data Subject Rights

10.1 The Processor shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests from Data Subjects exercising their rights under Chapter III of the GDPR, including but not limited to the right of access, rectification, erasure, restriction of processing, data portability, and the right to object.

10.2 If a Data Subject contacts the Processor directly with a request regarding their Personal Data, the Processor shall promptly forward such request to the Controller and shall not respond to the Data Subject directly unless instructed to do so by the Controller.

10.3 The Processor shall respond to the Controller's instructions regarding Data Subject requests within a reasonable timeframe to enable the Controller to comply with the applicable legal deadlines.

11. Data Retention and Deletion

11.1 Personal Data shall be retained by the Processor for the duration of the Agreement and processed in accordance with the Controller's documented instructions.

11.2 Upon termination or expiry of the Agreement, the Controller shall have a period of thirty (30) calendar days ("Export Window") to export all Personal Data and project data from the Application. The following export formats are available:

- **Project data:** DXF, DWG, JSON, CSV
- **User data:** CSV

11.3 After the expiration of the Export Window, the Processor shall permanently and securely delete all Personal Data within thirty (30) calendar days, unless retention of such data is required under applicable Union or Member State law.

11.4 Upon the Controller's written request, the Processor shall provide written confirmation that all Personal Data has been deleted in accordance with this Section.

11.5 Notwithstanding the foregoing, the Processor may retain Personal Data to the extent and for the period required by applicable law, provided that the Processor ensures the confidentiality of such Personal Data and that it is only processed as necessary for the purposes mandated by applicable law.

12. Audit Rights

12.1 The Controller, or a third-party auditor appointed by the Controller (subject to reasonable confidentiality obligations), may audit the Processor's compliance with this DPA, provided that:

(i) The Controller provides at least thirty (30) calendar days' prior written notice.

(j) The audit is conducted during the Processor's normal business hours.

(k) The audit is conducted at the Controller's expense.

(l) The audit does not unreasonably disrupt the Processor's business operations.

12.2 In lieu of an on-site audit, the Processor may, at its discretion, provide the Controller with:

- A summary or copy of relevant third-party audit reports, certifications, or assessments, provided that such reports are subject to confidentiality obligations.
- Written responses to the Controller's reasonable audit questions and compliance questionnaires.

12.3 Audits shall be limited to no more than one (1) per twelve (12) month period, unless a Personal Data Breach has occurred or there is a reasonable basis for the Controller to believe that the Processor is not in compliance with this DPA.

12.4 Any information disclosed to the Controller or its auditor during an audit shall be treated as confidential information of the Processor.

13. Liability

13.1 Each party's liability under this DPA is subject to the exclusions and limitations of liability set out in the Agreement.

13.2 The Processor shall not be liable for any processing of Personal Data that does not comply with the Controller's instructions, where the Processor has acted within or in accordance with the Controller's lawful documented instructions.

13.3 Nothing in this DPA shall limit or exclude either party's liability for damages caused by processing that does not comply with the GDPR, in accordance with Article 82 of the GDPR.

14. Term and Termination

14.1 This DPA shall become effective on the date the Controller first uses the Application (or, for existing Users, on the effective date stated above) and shall remain in force for as long as the Processor processes Personal Data on behalf of the Controller.

14.2 This DPA shall survive the termination or expiry of the Agreement and shall continue to apply until all Personal Data has been deleted or returned in accordance with Section 11 of this DPA.

14.3 The obligations imposed on the Processor under this DPA with respect to confidentiality, data security, and data breach notification shall survive the termination of this DPA.

Annex 1: Technical and Organizational Measures

This Annex describes the technical and organizational measures implemented by the Processor as of the effective date of this DPA. These measures are subject to periodic review and update in accordance with Section 8.

1. Access Control

- Application access control mechanisms, including (where applicable) role based access control (RBAC) with defined permission levels, ensuring that each user has access only to the data and functions necessary for their authorized use of the Application.
- The Processor manages user identity and access for the Application through Microsoft Entra (Microsoft Entra ID). The Application supports Single Sign On (SSO) via SAML 2.0 and OpenID Connect (OIDC), including sign in from external SAML/OIDC identity providers through federation with the Processor's Microsoft Entra tenant.
- Where agreed with the Client, System for Cross Domain Identity Management (SCIM) provisioning can be enabled via the Microsoft Entra provisioning service to automate the creation, update, and deprovisioning of user accounts in the Application.
- Within the Application, users are granted role based permissions, with administrative accounts able to manage the roles and administrative status of other users. Access to individual projects is controlled on a resource basis, allowing project owners to grant or revoke view and edit rights for other users within the Client's organization.
- Multi factor authentication (MFA), where applicable, is supported and available via Microsoft Entra.
- Minimum password requirements: twelve (12) characters with complexity requirements (uppercase, lowercase, digits, special characters).
- Configurable session timeout and automatic account lockout after repeated failed authentication attempts.
- Principle of least privilege applied across all access levels.

2. Encryption

- **Data in transit:** All data transmitted between the Application and end users is encrypted using Transport Layer Security (TLS) version 1.2 or higher.
- **Data at rest:** All Personal Data stored within the Application is encrypted using AES-256 encryption.
- **Database encryption:** Azure Transparent Data Encryption (TDE) is enabled for all databases.
- **Backup encryption:** All backups are encrypted at rest.

3. Infrastructure Security

- The Application is hosted on Microsoft Azure, utilizing EU-based data center regions (Ireland and the Netherlands).
- Network segmentation is enforced through Azure Network Security Groups (NSGs).
- Microsoft Defender for Cloud (formerly Azure Security Center) is utilized for continuous security posture management and threat detection.

4. Data Backup and Recovery

- Automated daily backups of all Application data, including Personal Data.
- Backup retention period: minimum seven (7) days.

- Point-in-time recovery capability with a Recovery Point Objective (RPO) not exceeding five (5) minutes.
- All backups are encrypted and stored in geo-redundant Azure storage within the EU.

5. Monitoring and Logging

- Application and user activity logs are retained for up to twelve (12) months.
- System and error logs are retained for the period necessary for operational and security purposes.
- Azure Monitor and Application Insights are deployed for performance monitoring and anomaly detection.
- Security event logging and real-time alerting for suspicious activities.

6. Incident Management

The Processor maintains documented incident response procedures with the following classification and response targets:

Classification	Description	Response Time	Resolution Target
P1 – Critical	Complete service outage or data breach	2 hours	24 hours
P2 – High	Major feature unavailable or significant performance degradation	4 hours	72 hours
P3 – Standard	Minor feature issues or cosmetic defects	8 hours	144 hours (6 business days)

- Post-incident review is conducted for all P1 and P2 incidents, with findings documented and corrective actions implemented.

7. Employee Security

- Background checks are performed for all personnel who handle or have access to Personal Data.
- All employees and contractors with access to Personal Data are bound by written confidentiality agreements.
- Regular security awareness training is provided to all staff.
- Access is granted based on role requirements, adhering to the principle of least privilege.

8. Physical Security

- Microsoft Azure data centers maintain comprehensive physical security controls, certified under SOC 1, SOC 2, and ISO 27001 standards, including biometric access controls, 24/7 surveillance, and on-site security personnel.
- RelineAI office premises are secured with locked access, visitor registration, and access control systems.

9. Vulnerability Management

- Regular vulnerability assessments and security scanning of the Application and its infrastructure.
- Annual penetration testing conducted by qualified third parties, with summary results available to the Controller upon request.
- Compliance with OWASP Top 10, targeting OWASP Application Security Verification Standard (ASVS) Level 2.
- Timely patching and remediation of identified vulnerabilities, prioritized by severity.

10. Business Continuity

- All source code is stored in version-controlled repositories with strict access controls.
- Automated deployment pipelines (CI/CD) ensure consistent and reliable application deployments.
- Azure Availability Zones are utilized for infrastructure redundancy and high availability.
- Documented disaster recovery procedures with defined recovery objectives.