Data Processing Agreement (sygnadesk)

VERSION	EFFECTIVE FROM	LANGUAGE
1.0	to be confirmed	Polski

In the event of any discrepancy between language versions, the Polski version prevails.

DRAFT FOR LEGAL REVIEW. Before publication this document requires review by a legal counsel or attorney.

This data processing agreement (the "DPA") forms an integral part of the agreement for the use of the sygnadesk service, concluded on the basis of the sygnadesk Terms of Service (the "Main Agreement"), and is entered into between the Client, acting as data controller (the "Controller"), and Jeton Cloud spółka z ograniczoną odpowiedzialnością spółka komandytowa, ul. Domaniewska 37/2.43, 02-672 Warsaw, Poland, KRS 0000850403, NIP 5213901362, REGON 386529721, acting as data processor (the "Processor"). Acceptance of the Terms of Service includes the conclusion of this DPA.

1. Subject matter, nature and purpose of processing

1.1. The Controller entrusts the Processor with the processing of personal data to the extent necessary to provide the sygnadesk service, that is, to make available and maintain a platform for receiving and handling reports of breaches of law and other irregularities, together with backups and technical support.

1.2. Processing is continuous and takes place in electronic form, for the term of the Main Agreement and for the data deletion period after its termination, described in section 7.

1.3. Categories of data subjects: persons making reports (insofar as they disclose their identity), persons to whom reports relate, persons named in the content of reports, and the Controller's Users to the extent of data recorded in connection with handling reports.

1.4. Types of data: identification and contact data, employment data, the content of reports and correspondence with the reporter, and attachments, which may include special categories of data within the meaning of Article 9 GDPR and data relating to breaches of law within the meaning of Article 10 GDPR, if included by the reporter or the Controller.

1.5. Account data of the Client and its Users (registration, billing, sign-in) is processed by Jeton Cloud as a separate controller and is not covered by this DPA; the rules for its processing are described in the privacy policy.

2. Controller's instructions and limits of processing

2.1. The Processor processes data solely on documented instructions from the Controller. The Main Agreement, the service configuration made by the Controller in the panel, and requests submitted by the Controller to technical support are deemed documented instructions.

2.2. The Processor does not use entrusted data for its own purposes, including analytics or marketing, and does not profile data subjects.

2.3. If, in the Processor's opinion, an instruction infringes data protection law, the Processor informs the Controller without delay.

3. Access to report content, two service modes

3.1. Standard mode. Report content is encrypted with keys managed by the platform. Access by the Processor's personnel to report content is restricted organisationally and technically and may occur only: at the Controller's express request in connection with handling a support ticket, or where mandatory provisions of law so require. Every such access is logged and the Controller is informed of it, unless the law prohibits this.

3.2. End-to-end encryption mode. Once this mode is enabled by the Controller, report content, attachments and correspondence are encrypted with keys held solely on the Controller's side. The Processor holds no key or recovery mechanism and has no technical ability to access this content, regardless of the basis of any request. In this mode, the Processor's activities with respect to the content are limited to storing and transmitting data in encrypted form.

3.3. Regardless of the mode, the Processor has access to technical data and metadata necessary to maintain the service (for example case identifiers, statuses, timestamps, billing data), which does not include report content.

4. Security and confidentiality

4.1. The Processor implements technical and organisational measures appropriate to the risk, in accordance with Article 32 GDPR, including: encryption of data in transit and at rest, access control and logging, separation of environments, regular encrypted backups stored with an independent provider in the European Economic Area in a form protected against premature deletion, automatic scanning of attachments for malicious software, and incident management procedures.

4.2. Only authorised persons bound by confidentiality under contract or statute are permitted to process data. The duty of confidentiality continues after those persons cease to work with the Processor.

5. Sub-processing

5.1. The Controller gives general consent to the Processor's use of further processors (sub-processors). The current list of sub-processors is available at https://sygnadesk.com/legal/subprocessors and forms part of this DPA.

5.2. The Processor informs the Controller of an intended addition or replacement of a sub-processor at least 14 days in advance, by updating the list and sending an email notice. The Controller may raise a reasoned objection within that period; failing agreement, either party may terminate the Main Agreement on the terms set out in the Terms of Service for adverse changes.

5.3. The Processor imposes on sub-processors data protection obligations no less stringent than those arising from this DPA and is liable for their acts as for its own.

5.4. Data is processed within the European Economic Area. Where a sub-processor's service involves a transfer outside the EEA, the transfer takes place on the basis of a valid mechanism under Chapter V GDPR (in particular standard contractual clauses), as noted in the list of sub-processors.

6. Assistance to the Controller and breaches

6.1. The Processor, taking into account the nature of the processing, assists the Controller in fulfilling the rights of data subjects and the obligations under Articles 32 to 36 GDPR, to the extent possible using the platform's functions and the information available to it. In end-to-end mode, assistance is limited to data the Processor can access.

6.2. The Processor notifies the Controller of a personal data breach concerning entrusted data without undue delay and no later than 36 hours after becoming aware of it, providing the information required by Article 33(3) GDPR as it becomes available.

6.3. Notifying the supervisory authority and communicating with data subjects remain the Controller's obligations.

7. End of processing

7.1. After termination of the Main Agreement the Processor, at the Controller's choice notified no later than 30 days after termination, returns the data in a commonly used format or deletes it. Absent an instruction, the data is deleted after that period.

7.2. Deletion also covers backups, which expire in accordance with the backup retention cycle of no more than 40 days from deletion of the data from the production system. Until they expire, backups remain encrypted and are not used for processing.

7.3. The Processor may retain data to the extent and for the period required by mandatory provisions of law.

8. Audit

8.1. The Controller may request information necessary to demonstrate compliance of the processing with Article 28 GDPR. The Processor first makes available documentation of security measures, descriptions of procedures, and any reports and certificates it holds.

8.2. An on-site audit, or an audit by an authorised auditor who is not a competitor of the Processor, is possible after agreeing a date at least 14 days in advance, during business hours, no more than once a year, unless the audit follows a breach. The Controller bears the cost of the audit. The audit may not compromise the confidentiality of the data of the Processor's other clients.

9. Liability and final provisions

9.1. The Processor's liability towards the Controller under this DPA is subject to the limitations set out in the Terms of Service, to the extent permitted by mandatory provisions of law, which do not limit liability towards data subjects arising directly from the GDPR.

9.2. This DPA remains in force for the term of the Main Agreement and the period described in section 7. Matters not regulated here are governed by the Terms of Service, the GDPR and Polish law.

Warsaw, [date to be completed]