Spotix Data Processing Agreement

Version 2026.12 · Effective 1 December 2026 · Signed version available on request (privacy@spotix.io)

At a glance

A summary for convenience. The full text below applies.

Topic	Summary	Clause
Roles	Customer is controller (or processor for its Clients); Cloud171 is processor (or sub-processor)	2
What is processed	Identity and configuration metadata from Microsoft 365 and Azure; no mailbox contents, files or chats	Annex I
Where	Stored and processed primarily in the EU (Germany and the Netherlands); traffic to the platform passes through Cloudflare's global network	8, Annex III
AI	Off by default; when enabled, only the limited data described in Annex I is sent to the AI model provider	4.4, Annex I, Annex III
Sub-processors	Published list; 30 days' notice of changes; right to object	7, Annex III
Personal data breaches	Notified to Customer without undue delay	10
End of service	Export, then deletion; credentials deleted within 5 business days	12
Audits	Documentation first; audits under conditions	13
Liability	As set out in section 15 of the Terms	14

1. Scope and precedence

1.1 This Data Processing Agreement ("**DPA**") forms part of the Agreement between Cloud171 B.V. ("**Cloud171**") and Customer, as defined in the Spotix Terms of Service ("**Terms**"). Capitalised terms not defined in this DPA have the meaning given in the Terms. The terms "personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "supervisory authority" have the meaning given in Regulation (EU) 2016/679 ("**GDPR**").

1.2 This DPA applies to the processing of personal data by Cloud171 on behalf of Customer in providing the Service ("**Customer Personal Data**"). It does not apply to personal data that Cloud171 processes as an independent controller, such as account, contact and billing data of Customer's users. For that data, Cloud171's Privacy Policy applies.

1.3 In the event of a conflict between this DPA and the Terms, this DPA prevails with respect to the processing of Customer Personal Data. Section 15 (Limitation of liability) and section 21 (Governing law and disputes) of the Terms always prevail, subject to Annex IV.

1.4 Customer accepts this DPA together with the Terms in the manner described in section 2.2 of the Terms. On request, Cloud171 will provide a version of this DPA for signature. A signed version has the same content as the version accepted online, unless the parties expressly agree otherwise in writing.

2. Roles of the parties

2.1 **Controller and processor.** With respect to Customer Personal Data, Customer is the controller and Cloud171 is the processor.

2.2 **Independent controller.** Cloud171 acts as an independent controller only for the personal data referred to in section 1.2.

2.3 **Customer acting as processor.** In the case of Managed Service Use (section 4.3 of the Terms), Customer acts as processor on behalf of its Clients and Cloud171 acts as sub-processor. In that case:

- (a) Customer warrants that its instructions to Cloud171, including the engagement of Cloud171 as sub-processor, have been authorised by the relevant controller;
- (b) Customer remains the sole point of contact for Cloud171. Cloud171 is not required to communicate directly with Clients, except where required by law;
- (c) references in this DPA to obligations of Customer as controller apply to Customer as processor. Customer will ensure that its Clients comply with the corresponding obligations of a controller;
- (d) Customer passes on to the Clients concerned, without undue delay, the notifications it receives from Cloud171 under this DPA, including notifications of sub-processor changes (section 7.3) and personal data breaches (section 10). Objections by Clients under section 7.4 are made through Customer.

3. Details of the processing

The subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subjects are described in **Annex I**.

4. Instructions

4.1 **Documented instructions.** Cloud171 processes Customer Personal Data only on the documented instructions of Customer, including with regard to transfers to a third country, unless Union or Member State law to which Cloud171 is subject requires otherwise. In that case, Cloud171 informs Customer of that legal requirement before the processing, unless that law prohibits such information on important grounds of public interest.

4.2 **Instructions given.** Customer's instructions consist of:

- (a) the Agreement, including this DPA;
- (b) the configuration and use of the Service by Customer, including connecting Tenants, starting scans and activating AI Features;
- (c) any further written instructions agreed by the parties.

Additional instructions that fall outside the scope of the Service require Cloud171's agreement and may be subject to additional fees.

4.3 **Anonymised data.** Customer instructs Cloud171 to create anonymised and aggregated data from the use of the Service, which do not identify Customer, any Tenant or any natural person, for the purposes of operating, securing and improving the Service (section 12.4 of the Terms). Cloud171 does not use Customer Personal Data for any other purpose of its own, and in particular does not use it to train AI models.

4.4 **AI Features.** AI Features are disabled by default (section 7 of the Terms). When an administrator of Customer activates AI Features, this constitutes an instruction to process the data described in Annex I, section 7. The AI model provider is listed in Annex III. Cloud171 logs each activation and deactivation.

4.5 **Unlawful instructions.** Cloud171 informs Customer immediately if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection law. Cloud171 may suspend the execution of the instruction concerned until Customer confirms or amends it. Cloud171 is not obliged to carry out a comprehensive legal review of Customer's instructions.

5. Confidentiality

Cloud171 ensures that persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Cloud171 grants access to Customer Personal Data only to the extent necessary for the performance of the Agreement.

6. Security

6.1 **Measures.** Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the risks to data subjects, Cloud171 implements appropriate technical and organisational measures in accordance with Article 32 GDPR. These measures are described in **Annex II**.

6.2 **Changes.** Cloud171 may update the measures in Annex II, provided that the overall level of security is not materially reduced. Cloud171 documents material changes.

6.3 **Customer's responsibility.** Customer is responsible for the security of its own environments, accounts and credentials, as described in sections 4 and 6 of the Terms. Customer has assessed the measures in Annex II and considers them appropriate for the processing under this DPA.

7. Sub-processors

7.1 **General authorisation.** Customer grants Cloud171 general written authorisation to engage sub-processors. The sub-processors engaged at the effective date of this DPA are listed in **Annex III**. Annex III is kept up to date in accordance with section 7.3 and always contains the current list. Previous versions are available via the version history.

7.2 **Obligations.** Cloud171 imposes on each sub-processor, by written contract, data protection obligations that meet the requirements of Article 28(3) GDPR. Cloud171 remains responsible to Customer for the performance of the obligations of its sub-processors in accordance with Article 28(4) GDPR, subject to section 14.

7.3 **Changes.** Cloud171 notifies Customer of any intended addition or replacement of a sub-processor at least thirty (30) days in advance, by email to Customer's administrator and/or by a notice in the Service. The notification includes the updated Annex III.

7.4 **Objection.** Customer may object to an intended change, on reasonable grounds related to data protection, by email to privacy@spotix.io within the notice period.

- (a) The parties will then consult in good faith about a solution.

- (b) If no solution is reached before the change takes effect, Customer may terminate the affected subscription with effect from the date of the change. In that case Cloud171 will refund any prepaid Fees for the remaining period on a pro-rata basis. This is Customer's sole remedy.
- (c) If Customer does not object within the notice period, it is deemed to have accepted the change.

7.5 **Urgent replacement.** If a sub-processor must be replaced urgently for reasons beyond Cloud171's control (for example the discontinuation of its service or a security risk), Cloud171 may make the replacement on shorter notice. In that case Customer's right of objection under section 7.4 applies from the date of notification.

8. International transfers

8.1 **Location.** Cloud171 stores and processes Customer Personal Data primarily in the European Union (database in Frankfurt, Germany; application servers in Amsterdam, the Netherlands). Traffic between users and the Service is routed through the global network of a content delivery and security provider, and may pass through data centres outside the EEA in transit. Annex III specifies the locations of each sub-processor.

8.2 **Transfers by Cloud171.** Cloud171 transfers Customer Personal Data to a country outside the EEA only if a valid transfer mechanism under Chapter V GDPR applies. This may be an adequacy decision (including, for certified US recipients, the EU-US Data Privacy Framework), or the Standard Contractual Clauses adopted by the European Commission (Decision (EU) 2021/914) with any necessary supplementary measures.

8.3 **Customers outside the EEA.** Where Customer is established in a country outside the EEA that is not covered by an adequacy decision, the transfer of Customer Personal Data by Cloud171 to Customer, such as making Output available or returning data, is governed by the Standard Contractual Clauses, **Module Four (processor to controller)**, or, where Customer acts as processor under section 2.3, **Module Three (processor to processor)**. These are incorporated into this DPA by reference, as further set out in **Annex IV**.

9. Assistance

9.1 **Data subject requests.** Cloud171 assists Customer, by appropriate technical and organisational measures and taking into account the nature of the processing, in responding to requests from data subjects to exercise their rights under Chapter III GDPR.

- (a) If Cloud171 receives such a request directly, it forwards the request to Customer without undue delay, and in any event within five (5) business days, if Cloud171 can identify Customer from the request.
- (b) Cloud171 does not respond to the request itself, except on Customer's instructions or where required by law.

9.2 **Other assistance.** Taking into account the nature of the processing and the information available to Cloud171, Cloud171 assists Customer in complying with its obligations under Articles 32 to 36 GDPR, including data protection impact assessments (DPIAs) and prior consultations.

9.3 **Costs.** Cloud171 provides the following assistance at no additional cost:

- (a) the standard information in this DPA and its Annexes;
- (b) the functionality of the Service, such as export and deletion;

- (c) standard answers to security questionnaires.

Cloud171 may charge for other assistance at its usual rates, unless the assistance is necessary because of a breach by Cloud171 of this DPA.

10. Personal data breaches

10.1 **Notification.** Cloud171 notifies Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data. Notification is made by email to Customer's administrator.

10.2 **Information.** The notification contains, to the extent then available:

- (a) the nature of the breach, including where possible the categories and approximate number of data subjects and records concerned;
- (b) the likely consequences;
- (c) the measures taken or proposed by Cloud171;
- (d) a contact point.

Where not all information is available at once, Cloud171 provides it in phases as it becomes available.

10.3 **Cooperation.** Cloud171 takes reasonable measures to contain the breach and mitigate its consequences. It cooperates with Customer to the extent necessary for Customer to meet its obligations under Articles 33 and 34 GDPR, and preserves relevant evidence.

10.4 **Notification to authorities and data subjects.** It is up to Customer, as controller, to assess whether a breach must be notified to the supervisory authority or to data subjects, and to make any such notification. Cloud171 does not notify supervisory authorities or data subjects of breaches affecting Customer Personal Data, unless required by law or agreed with Customer.

10.5 **No admission.** Notification of a personal data breach by Cloud171 does not constitute an admission of fault or liability.

11. Obligations of Customer

Customer:

- (a) ensures that it has a valid legal basis for the processing of Customer Personal Data through the Service, and that its instructions comply with the GDPR;
- (b) informs data subjects about the processing in accordance with Articles 13 and 14 GDPR;
- (c) carries out a data protection impact assessment where required, with Cloud171's assistance under section 9.2;
- (d) obtains any required approval from its works council or other employee representation. This applies in particular where the Service processes sign-in and usage data that could be used to monitor employees (for example under Article 27(1)(l) of the Dutch Works Councils Act, WOR);
- (e) is authorised to have the connected Tenants analysed, and manages the permissions and credentials granted to the Service in accordance with section 4 of the Terms;
- (f) does not instruct Cloud171 to process special categories of personal data or criminal data. The Service is not designed for such data;
- (g) notifies Cloud171 without undue delay if it becomes aware of a personal data breach or vulnerability relating to the Service.

12. Return and deletion

12.1 **During the Subscription Term.** Customer can export the exportable data described in section 11.2 of the Terms at any time. The metadata collected from Customer's Tenants remains available to Customer in those Tenants. Customer can delete reports and Tenants within the Service, after which the associated data are deleted from the production systems without undue delay, and from backups in accordance with section 12.3.

12.2 **After the end of the Subscription Term.**

- (a) Customer may retrieve its data during the retrieval period referred to in section 11.4 of the Terms.
- (b) Cloud171 deletes the credentials provided by Customer for its Tenants no later than five (5) business days after the end of the Subscription Term.
- (c) After the retrieval period, Cloud171 deletes all Customer Personal Data within thirty (30) days, unless Union or Member State law requires further storage. In that case Cloud171 informs Customer and limits processing to that storage.
- (d) For a trial that is not converted to a paid subscription, no retrieval period applies. Credentials are deleted within five (5) business days and Customer Personal Data within thirty (30) days after the end of the trial, in accordance with section 3.6 of the Terms.

12.3 **Backups.** Customer Personal Data in backups are deleted in the normal backup rotation cycle, no later than thirty (30) days after deletion from the production systems. Until then, backups are protected in accordance with Annex II and are not otherwise used.

12.4 **Confirmation.** On written request, Cloud171 confirms the deletion in writing within ten (10) business days of completing it.

13. Information and audits

13.1 **Information.** Cloud171 makes available to Customer, on reasonable request, all information necessary to demonstrate compliance with Article 28 GDPR and this DPA. This includes documentation of the measures in Annex II, answers to a reasonable security questionnaire and, where available, third-party audit reports or certifications.

13.2 **Audits.** Customer may audit compliance with this DPA, itself or through an independent auditor bound by confidentiality, if:

- (a) the information under section 13.1 is reasonably insufficient to demonstrate compliance;
- (b) a personal data breach affecting Customer Personal Data has occurred; or
- (c) a supervisory authority requires it.

13.3 **Conditions.** Audits under section 13.2 are subject to the following conditions:

- (a) at most once per calendar year, except in the cases of section 13.2(b) and (c);
- (b) at least thirty (30) days' prior written notice, with a proposed scope;
- (c) during normal business hours and with as little disruption as possible to Cloud171's operations;
- (d) no access to data of other customers, or to information that would compromise the security of the Service;
- (e) an auditor that is not a competitor of Cloud171;

- (f) Customer bears the costs of the audit, including Cloud171's reasonable internal costs at its usual rates;
- (g) Customer provides Cloud171 with a copy of the audit report free of charge, and treats the report as confidential information under section 13 of the Terms.

13.4 **Remediation.** If an audit reveals that Cloud171 does not comply with this DPA, Cloud171 will take reasonable measures to remedy the non-compliance within a reasonable period.

14. Liability

14.1 The liability of the parties under or in connection with this DPA is subject to section 15 of the Terms. This includes:

- (a) the cap;
- (b) the definition of direct damage;
- (c) the exclusion for free and trial use;
- (d) the requirement of a notice of default (*ingebrekestelling*) and the time limit.

14.2 Nothing in this DPA limits the rights of data subjects under Article 82 GDPR. As between the parties, including any recourse claim under Article 82(5) GDPR, section 15 of the Terms applies in full.

14.3 Administrative fines imposed on a party are borne by that party and cannot be recovered from the other party.

15. Term and termination

15.1 This DPA applies for as long as Cloud171 processes Customer Personal Data on behalf of Customer, including the retrieval period and the deletion period under section 12.

15.2 Sections 12, 13 (in respect of the period of processing), 14 and 16 survive the end of this DPA.

16. Governing law and disputes

This DPA is governed by Dutch law. Disputes are resolved in accordance with section 21 of the Terms, without prejudice to the rights of data subjects and supervisory authorities under the GDPR.

17. Contact

Cloud171 B.V., trading as Spotix
Steenovenweg 5, 5708 HN Helmond, the Netherlands
Chamber of Commerce: 91841755
Privacy contact: privacy@spotix.io

Annex I – Details of the processing

1. Subject matter
The provision of security, operations and cost insights for Customer's Microsoft 365 and Azure environments through the Spotix platform.

2. Duration
The Subscription Term, followed by the retrieval period and the deletion periods set out in section 12.

3. Nature of the processing

- Collecting metadata through the Microsoft Graph and Azure APIs, using the permissions that Customer grants.
- Storing and analysing that metadata.
- Assessing it against checks.
- Generating scores, findings and reports.
- Making Output available to Customer.
- Exporting and deleting data.
- If AI Features are enabled: sending the data described in section 7 of this Annex to the AI model provider.

4. Purpose
Providing the Service to Customer in accordance with the Agreement: insight into security configuration, identity hygiene, license use and costs, and supporting Customer's remediation.

5. Types of personal data

- *Identification data:* names, display names, user principal names (UPNs), email addresses.
- *Professional data:* job titles, departments, organisational structure, group memberships.
- *Technical identifiers:* object IDs, device names and identifiers, IP addresses where contained in the metadata.
- *License and activity data:* assigned licences, last sign-in and last-activity timestamps, MFA registration status.
- *Identity configuration:* role assignments, authentication methods, Conditional Access policies and exclusions.

The Service does **not** access or process mailbox contents, files, chat messages, calendar items or other user-generated content.

6. Categories of data subjects

- Customer's employees, contractors and other internal users.
- Guest users and external collaborators in Customer's Tenants.
- Persons associated with service accounts and technical identities.
- In the case of Managed Service Use: the corresponding persons at Customer's Clients.

7. AI Features (only if activated by Customer)
When AI Features are enabled, only the following data are sent to the AI model provider:

- (a) aggregated scores and counts per severity level and category;
- (b) aggregated savings totals and currency;
- (c) fixed check texts (title, severity, category, recommendation and remediation steps), as defined by Cloud171;
- (d) for remediation guidance: the summary of the relevant finding in Customer's Tenant. Such summaries may contain names of objects in the Tenant, such as Conditional Access policies, groups and access reviews, and, where relevant to the finding, display names of users or guests. These names may constitute personal data.

Credentials, sign-in data and complete user lists are never sent to the AI model provider. Under its commercial terms, the AI model provider does not use these data to train its models.

8. Special categories of personal data
None intended (see section 11(f)).

Annex II – Technical and organisational measures

The measures below describe the security approach of the Service. Cloud171 may update them in accordance with section 6.2.

Encryption

- Traffic between users and the Service is encrypted using TLS 1.2 or higher. HSTS is enforced.
- Traffic between the content delivery network and the application servers is also encrypted, and the origin certificate is validated.
- Data are encrypted at rest at the infrastructure level by the hosting providers.
- Credentials that Customer provides for its Tenants (client secrets and certificates) are additionally encrypted at the application layer before storage, and are accessible only to the components that need them to perform scans.

Network protection

- Protection against DDoS attacks and a web application firewall at the network edge.

Access to the Service

- Authentication via a specialised identity provider, with support for single sign-on and multi-factor authentication.
- Role-based access within Customer's organisation (administrator, analyst, viewer).

Segregation of customer data

- Customer data are logically segregated per organisation through access controls at application and database level.
- Background and scheduled processes are subject to the same segregation.

Minimisation

- The Service requests read-only permissions from Customer's Tenants, limited to those needed for the checks.
- Logging and error monitoring are configured to minimise personal data.
- AI Features are off by default and receive only the limited data described in Annex I, section 7.

Access by Cloud171 personnel

- Access to production systems is limited to authorised personnel on a need-to-know basis, protected by multi-factor authentication, and logged.
- Personnel are bound by confidentiality obligations.

Application security

- Security headers and a Content Security Policy.
- Rate limiting on authentication and sensitive endpoints.
- Dependency vulnerability scanning and timely patching.
- A public route for reporting vulnerabilities (security.txt and spotix.io/security).

Availability and continuity

- Hosting in EU data centres of recognised providers.
- Cloud171 uses hosting and infrastructure providers that maintain recognised security certifications or attestations, such as ISO/IEC 27001 and/or SOC 2.
- Regular backups with limited retention (see section 12.3 of the DPA).

Incident management

- A documented incident response procedure, including the assessment and notification of personal data breaches.
- An internal register of incidents.

Sub-processor management

- Written agreements with sub-processors meeting Article 28(3) GDPR.
- Periodic review of sub-processors' security.

Annex III – Sub-processors

Effective 1 December 2026. This Annex is updated in accordance with section 7.3.

Sub-processor	Purpose	Data	Location	Transfer mechanism
Neon, LLC (a Databricks company) / Databricks, Inc.	Database hosting (PostgreSQL)	All Customer Personal Data	EU (Frankfurt, Germany); support access by Databricks group personnel outside the EEA possible	EU-US Data Privacy Framework (Databricks, Inc., certified, including Neon, LLC); Standard Contractual Clauses (Module Three) under the Databricks DPA as fallback
Railway Corporation	Application hosting and compute	All Customer Personal Data (in processing)	EU (Amsterdam, the Netherlands); support access from the United States possible	EU-US Data Privacy Framework (certified); Standard Contractual Clauses (Module Three) under the Railway DPA as fallback

Sub-processor	Purpose	Data	Location	Transfer mechanism
Cloudflare, Inc.	Reverse proxy, content delivery, DDoS protection and web application firewall for the platform	All data transmitted between users and the platform, in transit (including Customer Personal Data displayed in or submitted to the platform), IP addresses and request metadata	Global edge network (Cloudflare, Inc., United States)	EU-US Data Privacy Framework (certified); Standard Contractual Clauses (Module Three) under the Cloudflare Data Processing Addendum as fallback
Functional Software, Inc. (Sentry)	Error and performance monitoring	Limited technical data; configured to minimise personal data	EU (Frankfurt, Germany) for event data; account and organisation metadata in the United States	EU-US Data Privacy Framework (certified); Standard Contractual Clauses (Module Three) under the Sentry DPA as fallback
Anthropic, PBC	AI Features: summaries and remediation guidance (only if activated by Customer)	The data described in Annex I, section 7, which may incidentally include personal data in Tenant object names	United States	Standard Contractual Clauses (Module Three) under Anthropic's Data Processing Addendum; no training on API data

For information:

- **Microsoft** is not a sub-processor of Cloud171. Customer Personal Data originate from Customer's own Microsoft 365 and Azure environments, which Customer uses under its own agreement with Microsoft.
- **Clerk** (authentication) and **Stripe** (payments) process account and billing data for which Cloud171 is an independent controller. See the Privacy Policy.

Annex IV – Standard Contractual Clauses (Module Four) for Customers outside the EEA

1. Where section 8.3 applies, the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, Module Four (transfer processor to controller) (the "**SCCs**"), are incorporated into this DPA by reference.
2. **Data exporter:** Cloud171 (processor). **Data importer:** Customer (controller). Where Customer acts as processor under section 2.3, Module Three applies instead, with Customer as data importer (processor) and the same options as set out in paragraph 3.
3. **Options:**
    - Clause 7 (docking clause) does not apply.
    - The optional wording in Clause 11 does not apply.
    - Clause 17: the SCCs are governed by the law of the Netherlands.
    - Clause 18: disputes are resolved by the courts of the Netherlands.
4. Annex I.A of the SCCs (list of parties) is completed with the details of the parties in the Agreement. Annex I.B (description of the transfer) is completed with Annex I of this DPA.
5. In the event of a conflict between the SCCs and this DPA, the SCCs prevail.

Signature (optional, for customers who want a signed version)

Customer	**Cloud171 B.V.**
Name:	Name:
Title:	Title:
Date:	Date:
Signature:	Signature:

Version history

Version	Date	Changes
2026.12	1 December 2026	Full revision: Article 28(3) GDPR requirements completed, TOMs in Annex II, sub-processor procedure with right to object, audit procedure, breach notification, Customer obligations, AI Features (opt-in), SCCs Module Four for customers outside the EEA, MSP and sub-processing roles.
2026.04	April 2026	First version.