Data Processing Agreement

pursuant to Article 28 GDPR

Version 1.1 – 19 November 2026 · Questions: shadowtrackr.com/contact

This Data Processing Agreement is entered into between the customer identified in the Main Agreement or order form (the **Controller**) and **ShadowTrackr Ltd**, a company incorporated in Cyprus (registration no. HE 488421, VAT no. CY60323384F) with its registered office at Kalymnou 1, “Q Merito” 4th Floor, Agios Nikolaos, 6037 Larnaca, Cyprus (the **Processor**, operating the ShadowTrackr service at shadowtrackr.com).

1. Background and scope

1.1 The Controller uses the ShadowTrackr External Attack Surface Management platform (the **Service**) under an agreement with the Processor (the **Main Agreement**).

1.2 In providing the Service, the Processor processes personal data on behalf of the Controller. This Data Processing Agreement (**DPA**) sets out the terms of that processing in accordance with Article 28 of Regulation (EU) 2016/679 (**GDPR**) and forms part of the Main Agreement.

1.3 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**.

2. Roles and instructions

2.1 The Controller is the controller and the Processor is the processor of the personal data processed under this DPA.

2.2 The Processor processes personal data only on documented instructions from the Controller, including with regard to transfers to a third country, unless required to do so by Union or Member State law. In that case the Processor informs the Controller of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.3 The Main Agreement, this DPA and the Controller’s use and configuration of the Service constitute the Controller’s complete instructions. The Processor informs the Controller without undue delay if it believes an instruction infringes the GDPR or other data protection law.

2.4 The Processor does not process the personal data for its own purposes. The Service performs passive reconnaissance only: it analyses publicly available information about the Controller’s internet-facing assets and does not actively probe, exploit or intrude upon systems.

3. Confidentiality

3.1 The Processor ensures that persons authorised to process the personal data are committed to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.2 Access to personal data is limited to personnel who need it to provide the Service and is protected by strong authentication.

4. Security of processing

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, the Processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as required by Article 32 GDPR.

4.2 The measures in force at the date of this DPA are described in **Annex II**. The Processor may update them, provided the overall level of security is not reduced.

5. Sub-processors

5.1 The Controller gives general written authorisation for the Processor to engage the sub-processors listed in **Annex III**.

5.2 The Processor informs the Controller of any intended addition or replacement of a sub-processor at least 30 days in advance (by email to the Controller's account contact or via the Service). The Controller may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Controller may terminate the affected part of the Service without penalty.

5.3 The Processor imposes on each sub-processor, by contract, data protection obligations no less protective than those in this DPA, and remains fully liable to the Controller for the sub-processor's performance.

6. International transfers

6.1 The Processor's core infrastructure and backups are located in the European Union, in Germany, at the Hetzner data centre in Nuremberg.

6.2 Where a sub-processor processes personal data outside the European Economic Area, the transfer takes place only on the basis of an adequacy decision, the EU Standard Contractual Clauses, or another transfer mechanism permitted by Chapter V GDPR, together with supplementary measures where required.

7. Assistance to the Controller

7.1 **Data subject rights.** Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organisational measures in responding to requests from data subjects. If the Processor receives such a request directly, it forwards it to the Controller without undue delay and does not respond itself unless instructed.

7.2 **Articles 32 to 36 GDPR.** The Processor assists the Controller in ensuring compliance with its obligations on security of processing, personal data breach notification, data protection impact assessments and prior consultation, taking into account the nature of processing and the information available to the Processor.

7.3 **Compliance frameworks.** The Processor provides reasonable information to support the Controller's obligations under NIS2 and comparable regulatory frameworks, to the extent they relate to the Service.

8. Personal data breaches

8.1 The Processor notifies the Controller without undue delay, and in any event within 24 hours, after becoming aware of a personal data breach affecting the Controller's personal data.

8.2 The notification includes, as far as known: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach and mitigate its effects. Information not yet available is provided in phases without undue further delay.

9. Return and deletion

9.1 On termination or expiry of the Main Agreement, the Controller may export its data during a **30-day grace period**.

9.2 After the grace period, the Processor deletes the Controller's personal data from production systems and scanner nodes, and purges it from backups, which are kept on a 30-day rolling basis, within 30

days of that deletion. Invoices, billing records and associated account details are retained for 7 years as required by tax law (Art. 52 EU VAT Directive). The Controller may request immediate deletion at any time; the Processor confirms deletion in writing within 5 business days.

10. Audits and information

10.1 The Processor makes available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR and allows for and contributes to audits, including inspections, conducted by the Controller or an auditor mandated by it.

10.2 The Processor will first satisfy audit requests through documentation, including this DPA, its security documentation, available third-party certifications of its infrastructure providers and, once obtained, its own certification reports. On-site audits require reasonable prior notice (at least 30 days), are limited to once per year unless a breach or regulatory request requires otherwise, take place during business hours without disrupting operations, and are subject to confidentiality obligations. Each party bears its own costs.

11. Liability

Liability under this DPA is governed by the liability provisions of the Main Agreement, without prejudice to the rights of data subjects under Article 82 GDPR.

12. Term, governing law and order of precedence

12.1 This DPA enters into force on the effective date of the Main Agreement and remains in force for as long as the Processor processes personal data on behalf of the Controller.

12.2 In case of conflict between this DPA and the Main Agreement concerning the processing of personal data, this DPA prevails.

12.3 This DPA is governed by the laws of Cyprus. The courts of Cyprus have exclusive jurisdiction, without prejudice to mandatory provisions of the GDPR.

Annex I – Description of the processing

Subject matter and purpose. Provision of the ShadowTrackr External Attack Surface Management Service: discovery, monitoring and reporting of the Controller's internet-facing assets and their security posture, including vulnerability (CVE) correlation, certificate and configuration monitoring, change alerting, and user and account administration.

Duration. For the term of the Main Agreement plus the 30-day export grace period described in section 9.

Nature of processing. Collection, storage, analysis, structuring, retrieval, alerting, reporting, export and deletion, performed with passive-only reconnaissance techniques.

Categories of data subjects

- Users and administrators of the Controller who have accounts in the Service
- Individuals whose personal data may appear incidentally in public information about the Controller's assets (for example, contact names or email addresses in certificates, WHOIS or DNS records, or on public web pages)

Types of personal data

- Account data: name, business email address, role, authentication data (bcrypt password hashes, TOTP secrets, passkey public keys, API keys and session data)
- Usage and technical data: IP addresses, access and audit logs, notification and alert settings
- Asset data that may contain personal data: domain names, IP addresses, certificate subject details, public contact details and email addresses found in public records
- Support communications between the Controller's users and the Processor

Special categories of data

None are intentionally processed.

Annex II – Technical and organisational measures (TOMs)

The measures below describe the Processor's security controls at the date of this DPA.

1. Information security governance

- Documented information security policy and an information security management system (ISMS) aligned to ISO/IEC 27001. Formal ISO/IEC 27001 certification of the Processor is in progress and is not claimed at the date of this DPA.
- Alignment with the Dutch BIO2 baseline and NIS2 requirements.

2. Access control and authentication

- Least-privilege, role-based access to production systems and personal data. Access to production systems is restricted to a minimal set of personnel and all administrative access is logged.
- Phishing-resistant authentication (passkeys) for staff access.
- Role-based access for customer users (administrator, user and read-only user).
- Customer authentication by email and password with optional multi-factor authentication (TOTP or passkey) and API keys; sessions are invalidated server-side on logout and account deletion.
- Single sign-on via OpenID Connect (Microsoft Entra ID, Okta, Keycloak and other OIDC providers) is available, with an option to require SSO and disable password login.
- Scoped API keys with administrative, regular and read-only access levels.
- Access is revoked promptly when personnel leave or change roles.

3. Encryption and data protection

- Encryption of data in transit using TLS 1.2 as a minimum (TLS 1.3 preferred) for web and API traffic, and TLS with certificate pinning between scanner nodes and core infrastructure.
- AES-256 encryption of data at rest on core infrastructure; backups encrypted with AES-256 and stored in Germany; AES-256 full-disk encryption on scanner nodes. SSO client secrets are encrypted at rest.
- Passwords stored using bcrypt hashing.

4. Infrastructure and physical security

- Core infrastructure and backups hosted in Germany at Hetzner Online GmbH (ISO/IEC 27001:2022, BSI C5 Type 2). Scanner nodes run on Hetzner and on Akamai Cloud (Linode; ISO 27001, SOC 2 Type 2, BSI C5). Physical access controls are provided by the data centre operator.
- Network segmentation, firewalling and hardened configuration of production systems. Scanner nodes store no customer data, are isolated from core infrastructure and are administered only over SSH with key-based authentication (password login disabled).

5. Data minimisation and passive reconnaissance

- The Service uses passive-only reconnaissance and does not actively exploit or intrude on target systems.
- Only data needed to deliver the Service is collected and retained. Customer data is not used to train machine learning models and is not provided to third-party AI services.

6. Logging, monitoring and incident response

- Logging of administrative and security-relevant events.
- Internal monitoring and alerting for availability, disk, API and CI failures, routed to the operations team.
- Documented incident and personal data breach response procedure with notification as set out in section 8.

7. Availability and resilience

- Encrypted backups kept on a 30-day rolling basis and stored in Germany.
- Ability to restore data from backup, tested after incidents.

8. Software development and change management

- Version-controlled code, change review and automated testing in CI before release.
- Dependencies are monitored for known CVEs and updated promptly. The Processor's own assets are continuously scanned with ShadowTrackr, and critical and high findings are treated as production incidents.

9. Personnel

- Confidentiality obligations for all personnel with access to personal data.
- Security awareness expectations for staff.

10. Data retention and deletion

- Documented data retention policy, with a 30-day export grace period after termination and subsequent deletion as set out in section 9.

11. Supplier management

- Sub-processors are selected for their security posture and bound by data processing terms (see Annex III).

Annex III – Authorised sub-processors

Sub-processor	Purpose	Location of processing	Transfer mechanism
Hetzner Online GmbH	Hosting of core infrastructure, database and backups	Nuremberg, Germany (EU) for core infrastructure and backups; scanner nodes may also run in Falkenstein, Germany (EU)	Not applicable (EU)
Akamai Cloud (Akamai Technologies, Inc. / Linode)	Hosting of scanner nodes (no customer data is stored; scan results are transmitted encrypted to core infrastructure)	Various locations worldwide	No customer data stored; EU SCCs under the Linode DPA where applicable
Stripe Payments Europe, Ltd.	Credit card payment processing for subscriptions (only for customers paying by credit card)	Ireland (EU), with possible processing in the US	EU–US Data Privacy Framework; EU SCCs as fallback (Stripe Data Transfers Addendum)
Microsoft Ireland Operations Ltd. (Microsoft 365 / Exchange Online)	Business email and support communications (tenant located in Cyprus, EU)	EU	EU Data Boundary; EU–US Data Privacy Framework and EU SCCs under the Microsoft DPA
Superlative Enterprises Pty Ltd (Have I Been Pwned)	Data breach exposure check of email addresses found on the Controller's assets. Enabled by default, using ShadowTrackr's own HIBP key and sending full email addresses. The Controller can opt out, or use its own HIBP API key with k-anonymity enabled (only hash prefixes are sent, and HIBP is then the Controller's own supplier).	Australia (operator); hosted in the United States (Microsoft Azure, West US)	EU SCCs under the HIBP Data Processing Addendum

Akamai Cloud (Linode) operates its services from third-party data centres, including Equinix and Telstra facilities; these are Akamai's own sub-processors.

Optional integrations

The Service also offers integrations with third-party services. These are switched off by default and are activated only by the Controller (opt-in).

Censys, Inc. (Ann Arbor, Michigan, USA) and Shodan (Seattle, Washington, USA). When the Controller enables the integration, the IP addresses, subnets, URLs and domains of the Controller's assets that the Service has discovered for the Controller are sent to the provider as lookup queries to enrich the Controller's own data, and the provider returns its own data about them. These providers act as sub-processors for that integration only. The data sent is limited to identifiers of the Controller's own, publicly exposed assets. Censys's privacy policy provides for transfers to the United States under a data processing agreement incorporating standard data protection clauses; Shodan does not publish a data processing agreement or a transfer mechanism. The Controller enables each integration on its own instruction and at its own discretion, and can disable it at any time.

The Shadowserver Foundation (Milpitas, California, USA). The Controller registers its own networks directly with Shadowserver, and the Service only retrieves the resulting reports. The Processor sends no personal data to Shadowserver, so Shadowserver is not a sub-processor of the Processor.

The Processor will notify the Controller of changes to this list as set out in section 5.2.