DarkStrata

LEGAL

Data Processing Agreement

Version 1.0

Effective 1 September 2026

Terms under which DarkStrata Ltd processes personal data on behalf of its customers, as required by Article 28 of the UK GDPR and the EU GDPR.

1. Background and scope

This Data Processing Agreement ("DPA") forms part of the agreement between DarkStrata Ltd ("DarkStrata", "we") and the customer identified in the applicable order or account registration ("Customer", "you") for the DarkStrata credential and dark-web monitoring services (the "Services") (together, the "Agreement").

It applies where DarkStrata processes Personal Data on the Customer's behalf in the course of providing the Services and sets out the terms required by Article 28 of the UK GDPR and, where applicable, the EU GDPR.

In the event of conflict between this DPA and the rest of the Agreement, this DPA prevails in respect of the processing of Personal Data.

2. Definitions

- "Data Protection Law" means the UK GDPR, the Data Protection Act 2018, and where the Customer is established in the European Economic Area, Regulation (EU) 2016/679 (the "EU GDPR"), each as amended.
- "Customer Data" means Personal Data that DarkStrata processes on the Customer's behalf, as described in Annex 1.
- "Data Corpus" means DarkStrata's independently collected dataset of breached, leaked and infostealer-derived records, which DarkStrata controls in its own right.
- "Subprocessor" means a third party engaged by DarkStrata to process Customer Data.
- "Controller", "Processor", "Personal Data", "Data Subject", "Personal Data Breach" and "processing" have the meanings given in Data Protection Law.

3. Roles of the parties

For Customer Data, the Customer is the Controller and DarkStrata is the Processor. Where the Customer acts on behalf of its own clients (for example as a managed service provider or reseller), the Customer warrants that it is authorised to appoint DarkStrata as a Processor or Sub-processor on those clients' behalf.

For the Data Corpus, DarkStrata is an independent Controller. Matching the Customer's monitored assets against the Data Corpus is a processing activity DarkStrata performs as Processor; the Data Corpus itself, and DarkStrata's collection and retention of it, are outside the scope of this DPA and are governed by DarkStrata's Privacy Policy.

4. Processing on instructions

DarkStrata processes Customer Data only on the Customer's documented instructions, which are: the Agreement, this DPA, and the Customer's configuration and use of the Services (including monitored assets, alert rules and integrations). DarkStrata will inform the Customer if, in its opinion, an instruction infringes Data Protection Law.

DarkStrata will not process Customer Data for any other purpose, including for model training, benchmarking or resale, and will not add Customer Data to the Data Corpus.

5. Confidentiality

DarkStrata ensures that personnel authorised to process Customer Data are bound by written confidentiality obligations and receive appropriate data protection training. Access is restricted to personnel who need it to provide, support or secure the Services.

6. Security

DarkStrata implements and maintains the technical and organisational measures described in Annex 2, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, so as to ensure a level of security appropriate to the risk.

DarkStrata may update those measures from time to time provided the overall level of security is not reduced.

7. Subprocessors

The Customer gives DarkStrata general written authorisation to engage the Subprocessors listed in Annex 3, which is maintained at darkstrata.io/en/subprocessors/. DarkStrata imposes data protection obligations on each

Subprocessor that are no less protective than those in this DPA and remains liable for the Subprocessor's performance.

DarkStrata will give the Customer at least 30 days' notice by email before a new Subprocessor processes Customer Data. The Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection in good faith, the Customer may terminate the affected Services and receive a pro-rata refund of any prepaid fees.

8. International transfers

Customer Data is stored and processed in the United Kingdom. DarkStrata's hosting infrastructure is located in London and is listed in Annex 3.

Customers established in the EEA: the United Kingdom benefits from an adequacy decision of the European Commission under Article 45 of the EU GDPR. Transfers of Customer Data to DarkStrata therefore require no additional transfer mechanism.

Where a Subprocessor processes Customer Data outside the United Kingdom or EEA, DarkStrata ensures the transfer is covered by an adequacy regulation, the UK International Data Transfer Agreement or Addendum, or another mechanism valid under Data Protection Law, as recorded in Annex 3.

9. Assistance to the Customer

Taking into account the nature of the processing, DarkStrata will assist the Customer by appropriate technical and organisational measures in responding to Data Subject requests (access, rectification, erasure, restriction, portability and objection). Where a Data Subject contacts DarkStrata directly about Customer Data, DarkStrata will refer the request to the Customer without undue delay and will not respond except on the Customer's instruction or as required by law.

DarkStrata will assist the Customer in meeting its obligations regarding security, Personal Data Breach notification, data protection impact assessments and prior consultation with a supervisory authority, taking into account the information available to DarkStrata.

10. Personal Data Breach

DarkStrata will notify the Customer without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting Customer Data. The notification will describe the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed, and a point of contact. Information may be provided in phases as it becomes available.

11. Deletion and return

On termination or expiry of the Agreement, or on the Customer's written request, DarkStrata will delete Customer Data within 90 days, save to the extent retention is required by law. Before deletion the Customer may export its Customer Data through the Services or the API. Backups are overwritten in the ordinary course within the same period.

12. Audit

DarkStrata will make available to the Customer all information reasonably necessary to demonstrate compliance with this DPA, including security documentation and certifications. DarkStrata will allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer, no more than once in any 12-month period unless required by a supervisory authority or following a Personal Data Breach, on at least 30 days' written notice, during business hours, and subject to reasonable confidentiality and scope limitations.

13. Liability, term and governing law

Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement. This DPA remains in force for as long as DarkStrata processes Customer Data. It is governed by the laws of England and Wales, save that where the Customer is established in the EEA, the mandatory provisions of the EU GDPR apply to the processing.

Annex 1. Details of processing

Item	Description
Subject matter	Provision of credential, infostealer and dark-web exposure monitoring for the Customer's domains, identities and assets.
Duration	The term of the Agreement plus the deletion period in section 11.
Nature and purpose	Storing the Customer's monitored assets; matching them against the Data Corpus; generating, storing and delivering alerts, reports and summaries; delivering data to Customer-configured integrations; account administration, billing and support.
Categories of Data Subjects	The Customer's employees, contractors and administrators; individuals whose identifiers the Customer monitors (for example staff or executives); the Customer's own clients where the Customer resells the Services.
Categories of Personal Data	Names, business email addresses and roles of account users; monitored domains, email addresses and other identifiers; exposure findings relating to those identifiers (including breached or leaked credentials, device and malware details); alert history; audit logs; billing contact details.
Special category data	None intentionally processed. Exposure findings may incidentally reveal information about a Data Subject's accounts or devices.

Annex 2. Technical and organisational measures

- Encryption in transit (TLS 1.2 or higher) on all external and internal service connections, and encryption at rest for databases, object storage and backups.
- Customer Data hosted in ISO 27001 certified data centres in the United Kingdom, with logical tenant isolation enforced at the application and database layer.
-

Role-based access control for Customer users; per-key scoped permissions for API access; multi-factor authentication available for all accounts.

- Administrative access to production limited to named DarkStrata personnel, over an authenticated private network, with all access logged.
- Network segmentation between public-facing services and internal processing; web application firewall and DDoS protection at the edge.
- Secrets managed in encrypted configuration; no credentials in source control.
- Centralised logging and error monitoring with alerting; regular review of security events.
- Automated daily backups of the primary database with point-in-time recovery; off-site backup of the Data Corpus in a separate provider.
- Dependency and vulnerability scanning in the build pipeline; security-relevant changes reviewed before deployment.
- Documented incident response procedure covering triage, containment, Customer notification and post-incident review.
- Cyber Essentials certification maintained.
- Data protection and security awareness training for all personnel with production access.

Annex 3. Subprocessors

The current list of Subprocessors, their location and the transfer safeguard relied on is published at darkstrata.io/en/subprocessors/ and is incorporated into this DPA. The list as at 1 September 2026 is:

Subprocessor	Purpose	Location
DigitalOcean, LLC	Application and database hosting	United Kingdom (London)
Amazon Web Services EMEA SARL	Data storage and processing	United Kingdom (London)
Cloudflare, Inc.	Network delivery, security and backup	Global edge network; backups stored in Western Europe

Resend, Inc.	Email delivery	European Union (Ireland)
Stripe Payments Europe, Ltd.	Payments and invoicing	European Union and United States
Functional Software, Inc. (Sentry)	Error monitoring	European Union (Germany)
Anthropic, PBC	AI summaries of exposure findings	United States
GitHub, Inc.	Software delivery	United States
Tailscale Inc.	Private networking	Canada and United States

Signatures

Signature is optional: this DPA applies to every customer account by incorporation into the Terms & Conditions.

Customers who require a countersigned copy may complete this page.

DARKSTRATA LTD

Signed

Name

Title

Date

CUSTOMER

Signed

Name

Title

Date