Data Processing Agreement

Pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR) · Version 2.3 (final), June 2026

1. The Parties

The Processor. RevealMyRisk — Herr Godfrey Mwasanje, Cybersecurity & Artificial Intelligence, Block Services | Mail handling, Stuttgarter Straße 106, 70736 Fellbach, Germany, contact@revealmyrisk.com, operating the service “RevealMyRisk” (revealmyrisk.com), represented by Godfrey Mwasanje, Owner (hereinafter “RevealMyRisk” or the “Processor”).

The Controller. The customer entity subscribing to the RevealMyRisk service, identified as follows (to be completed by the Controller):

Field	To be completed by the Controller
Legal entity name	
Company registration no.	
Registered address	
Represented by (name, title)	

The Processor and the Controller are individually a “Party” and collectively the “Parties”.

2. Background and Scope

2.1 The Controller has subscribed to the RevealMyRisk service (the “Service”), under which the Processor provides a credential-exposure monitoring and threat-intelligence platform.

2.2 In the course of providing the Service, the Processor processes personal data on behalf of the Controller, namely the Controller’s account and usage data (e.g. user login credentials, monitored domains, billing information and support communications). This DPA governs that processing.

2.3 **Distinct controllership over indexed data.** Separately from this DPA, RevealMyRisk acts as an independent controller in respect of the compromised-credential datasets it indexes or licenses from publicly available breach and leak sources, including the surfacing of exposure results matching a domain or asset. That activity is carried out under RevealMyRisk’s own controllership and legal basis and does not fall within the scope of this DPA; the Controller has no controllership, instruction rights or responsibility over those datasets.

2.4 In the event of conflict between this DPA and the Terms of Service or other service agreement between the Parties (the “Main Agreement”), this DPA prevails with respect to the processing of personal data.

3. Definitions

Terms such as “personal data”, “processing”, “data subject”, “controller”, “processor”, “sub-processor” and “personal data breach” have the meanings given to them in the GDPR. “Applicable Data Protection Law” means the GDPR and any national legislation implementing or supplementing it, including the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG).

4. Subject Matter and Duration of Processing

4.1 The subject matter, nature, purpose and duration of the processing, the types of personal data and the categories of data subjects are described in Annex 1.

4.2 This DPA forms an integral part of the Main Agreement and is incorporated into it by reference. It is binding without separate signature: it takes effect on the Controller’s acceptance of the Main

Agreement or first use of the Service, whichever is earlier, and remains in force for as long as the Processor processes personal data on behalf of the Controller. The Processor's signature is pre-applied to the published version; the signature blocks in Section 11 are provided for Controllers requiring a counter-signed copy.

5. Obligations of the Processor

The Processor shall:

- Process personal data only on documented instructions from the Controller, including with regard to transfers, unless required otherwise by Union or Member State law; in such a case the Processor informs the Controller before processing, unless prohibited on important grounds of public interest. The Main Agreement, this DPA and the Controller's configuration and use of the Service constitute the Controller's documented instructions.
- Ensure that persons authorised to process the personal data are bound by confidentiality or an appropriate statutory obligation of confidentiality.
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in Annex 3, in accordance with Article 32 GDPR.
- Respect the conditions for engaging sub-processors set out in Section 6.
- Assist the Controller, by appropriate technical and organisational measures and insofar as possible, in responding to data subject requests under Chapter III GDPR.
- Assist the Controller in ensuring compliance with Articles 32 to 36 GDPR (security, breach notification, data protection impact assessments and prior consultation), taking into account the nature of processing and the information available to the Processor.
- At the choice of the Controller, delete or return all personal data after the end of the provision of the Service and delete existing copies, unless Union or Member State law requires storage (see Section 9).
- Make available all information necessary to demonstrate compliance with Article 28 GDPR and allow for and contribute to audits, subject to Section 8.

The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Applicable Data Protection Law.

6. Sub-processors

6.1 The Controller grants the Processor general written authorisation to engage the sub-processors listed in Annex 2 for the performance of the Service.

6.2 The Processor shall inform the Controller of any intended addition or replacement of a sub-processor at least thirty (30) days in advance, giving the Controller the opportunity to object. If the Controller objects on reasonable data-protection grounds, the Parties shall discuss the objection in good faith. If no alternative is agreed within a reasonable period, the Controller may terminate the affected Service without penalty by written notice, with a pro-rata refund of prepaid fees for the unused portion of the subscription term.

6.3 Sub-processors are engaged under a contract imposing data-protection obligations substantially equivalent to those in this DPA. The Processor remains fully liable to the Controller for the performance of the sub-processor's obligations.

7. International Transfers

7.1 Core account and monitoring data is hosted within the EU/EEA. Where a sub-processor is established outside the EEA, transfers take place only on the basis of an adequacy decision (including the EU-U.S. Data Privacy Framework where applicable) or the Standard Contractual Clauses adopted by

the European Commission, together with any supplementary measures required following a transfer impact assessment.

7.2 Where the Controller configures outbound delivery channels (for example webhooks or third-party messaging tools) that are located outside the EEA, the resulting transfer is carried out on the Controller's instruction and under the Controller's responsibility. The Processor does not pre-validate or geolocate destinations chosen by the Controller.

8. Personal Data Breach and Audit

8.1 **Breach notification.** The Processor notifies the Controller without undue delay and in any event within twenty-four (24) hours of becoming aware of a personal data breach affecting the Controller's personal data, and provides a substantive update containing the information referred to in Article 33(3) GDPR within a further forty-eight (48) hours, to the extent then available.

8.2 **Audit.** The Controller may audit the Processor's compliance with this DPA once per twelve-month period, and additionally following a personal data breach affecting the Controller's data, on at least thirty (30) days' written notice, during business hours and subject to confidentiality. The Processor may satisfy an audit request by providing existing documentation, certifications or reports where these reasonably address the scope of the request. Costs of an audit are borne by the Controller, save where the audit reveals a material breach of this DPA.

9. Return and Deletion of Data

9.1 Upon termination of the Service, the Processor deletes or anonymises the Controller's account and monitoring personal data within ninety (90) days, save for data that must be retained to comply with a legal obligation (for example billing records retained under German commercial and tax law). Within the same period the Processor provides a written deletion certificate identifying any data retained on legal grounds and the corresponding retention period.

9.2 Upon the Controller's written request made before the end of that period, the Processor shall instead return the personal data in a commonly used format and then delete it.

10. Liability and Miscellaneous

10.1 Notwithstanding any limitation of liability in the Main Agreement, each Party's aggregate liability under this DPA is capped at an amount equal to ten (10) times the fees paid or payable by the Controller during the twelve (12) months preceding the event giving rise to the claim. This cap does not apply to liability that cannot be excluded or limited under applicable law, including liability arising from intent or gross negligence.

10.2 This DPA is governed by German law. The courts competent for the Processor's place of business have exclusive jurisdiction, to the extent permitted by law.

10.3 The Processor may update this DPA to reflect changes in law, sub-processors or the Service, provided the level of protection is not diminished; material changes are notified at least thirty (30) days in advance.

10.4 If any provision of this DPA is held invalid or unenforceable, the remaining provisions remain in full force and effect.

11. Signatures

This DPA is binding on both Parties through its incorporation into the Main Agreement (Section 4.2). Signature below is optional and provided for Controllers that require a counter-signed copy. The Processor's signature is pre-applied to the published version.

For the Processor (RevealMyRisk)	For the Controller
Name: Godfrey Mwasanje	Name: _____
Title: Owner	Title: _____
Date: June 2026	Date: _____
Signature: /s/ Godfrey Mwasanje	Signature: _____

Annex 1. Description of the Processing

Item	Description
Subject matter	Processing of the Controller's account and usage data necessary to provide the RevealMyRisk credential-exposure monitoring service.
Nature and purpose	Account creation and authentication; configuration and monitoring of the Controller's designated domains and assets; generation of exposure results, alerts and reports; billing; and customer support.
Duration	For the duration of the Main Agreement, followed by deletion or anonymisation in accordance with Section 9 (within 90 days of termination, subject to legal retention obligations).
Categories of data subjects	The Controller's authorised users and administrators of the Service.
Categories of personal data	Account data: name, business email, login credentials (hashed), role. Configuration data: monitored domains and assets. Billing data: billing contact, company details, transaction records. Support data: contact details and correspondence. Technical data: IP address, device fingerprint hash, log and usage metadata.
Special categories	None are intentionally processed. The Service is not designed to process special categories of personal data under Article 9 GDPR.

Annex 2. Authorised Sub-processors

The following sub-processors are authorised to process the Controller's personal data in connection with the Service:

#	Sub-processor	Purpose	Location	Transfer mechanism
1	Managed application hosting and edge delivery platform	Hosting of the web application and server functions	EU/EEA	Intra-EU/EEA
2	Managed database, authentication and storage platform	Account data, authentication, audit logs, backups	EU/EEA (Germany)	Intra-EU/EEA
3	Transactional email provider	Delivery of account, credential and notification emails	EU/EEA or adequacy country	Intra-EU/EEA, adequacy decision or SCCs
4	Upstream breach-intelligence data provider	Supply of exposure datasets queried through the Service	EU/EEA	Intra-EU/EEA

Note 1. Core account and monitoring data is stored within the EU/EEA.

Note 2. Where the Controller activates outbound channels it operates itself, the destination of those payloads is determined by the Controller.

Note 3. The exact corporate entity, country of establishment and applicable transfer mechanism for each sub-processor may be confirmed on request. The Processor notifies the Controller of any addition or replacement at least thirty (30) days in advance in accordance with Section 6.2.

Annex 3. Technical and Organisational Security Measures

Pursuant to Article 32 GDPR, the Processor implements the following measures, appropriate to the nature, scope and purpose of the processing carried out for the Controller and to the risks for the rights and freedoms of natural persons. A fuller description is published on the RevealMyRisk security page.

Encryption and data transmission

- Encryption of data in transit using TLS 1.2 or higher (TLS 1.3 preferred) for all connections to the Service, its interfaces and between infrastructure components.
- Encryption of production data and backups at rest using AES-256.
- Login passwords stored exclusively as salted cryptographic hashes; plaintext passwords are never retained.
- Upstream connection credentials stored server-side only and never transmitted to the browser.

Access control and authentication

- Role-based access control restricting access to personal data to authorised personnel on a need-to-know basis.
- Row-level security policies enforced at the database engine for all customer-scoped tables.
- Sessions bound to an approved device by way of a non-reversible device fingerprint hash.
- Multi-factor authentication enforced on administrative and infrastructure access.
- Periodic review of access rights; removal of access on personnel or role changes.

Infrastructure and segregation

- Controller account and monitoring data hosted within EU/EEA data centres.
- Production environments logically isolated from development and preview environments.
- Changes reach production only through a controlled deployment pipeline.

Resilience and continuity

- Regular encrypted backups of production data with point-in-time restore capability.
- Monitoring and append-only logging of privileged access and system events.

Incident response and organisational measures

- Documented incident response procedure including breach notification under Section 8.
- Confidentiality commitments binding all personnel with access to personal data.
- Sub-processors engaged only under data-protection obligations equivalent to those in this DPA.
- Periodic review of technical and organisational measures and of automated security scanning results.