DATA PROCESSING AGREEMENT ("Agreement")

Last updated 22 April 2025 – Draft v0.9
This template is provided for discussion purposes only and does not constitute legal advice. Horizon Landings Ltd (trading as "Rivelin") recommends that each Customer obtain its own legal counsel before execution.

---

1 Parties

Party	Role	Details
Horizon Landings Ltd (trading as **"Rivelin"**) Registered office: TBC Email: privacy@rivelin.io	*Processor*	Registered in England & Wales (Company No. TBC)
Customer	*Controller*	Entity identified in the Order Form or online sign-up.

Together referred to as the **"Parties."**

---

2 Definitions

Terms *Controller*, *Processor*, *Data Subject*, *Personal Data*, *Processing*, *Personal Data Breach* and *Supervisory Authority* have the meanings set out in Article 4 UK GDPR.

---

3 Purpose & Nature of Processing

Item	Description

Service	API-based and bulk-file services for email, phone and address verification, optional IP fraud risk scoring (“Services”).
Operations	Collection, hosting, pseudonymisation (hashing), validation, enrichment, scoring, storage, retrieval, deletion.
Categories of Data *	Email addresses, phone numbers, IP addresses, postal addresses, customer IDs or reference keys.
Data Subjects	End-customers, leads and other individuals supplied by Controller.
Retention Period	**Controller-defined** via API parameter or dashboard (default 30 days); Processor deletes or irreversibly pseudonymises data when retention ≠ 0 expires.

** The Services function on hashed representations where practicable (e.g. SHA-256 of email) to minimise direct identifiers in storage.*

---

4 Duration

This Agreement is coterminous with the Master SaaS Agreement. Processing continues for the subscription term plus **90 days** for graceful shutdown unless earlier instructed to delete.

---

5 Processor Obligations

1. **Instructions.** Process Personal Data only on documented instructions from Controller, including with respect to transfers.
2. **Confidentiality.** Ensure personnel are bound by confidentiality.
3. **Security Measures.** Maintain the technical & organisational measures in *Schedule 1*.
4. **Sub-processors.** Engage only those in *Schedule 2*; give 15 days’ notice before replacement.
5. **Data Subject Rights.** Assist Controller in fulfilling requests under Articles 15-22 UK GDPR.
6. **Breach Notification.** Notify Controller without undue delay (≤ 24 h) after becoming aware of a Personal Data Breach.
7. **Deletion / Return.** Upon request or termination, delete or return Personal Data except as required by law.
8. **Audits.** Provide up-to-date third-party audit reports (Cyber Essentials Plus; ISO 27001 once achieved) and allow onsite inspection with 30 days’ notice.

6 Controller Obligations

1. Ensure all Personal Data provided is collected lawfully.
2. Configure retention settings consistent with legal obligations.
3. Provide breach notifications to Supervisory Authorities and Data Subjects where required.
4. Maintain secure authentication (MFA) for all user accounts.

7 International Transfers

Personal Data is stored in **Amazon Web Services eu‑west‑2 (London)** and **eu‑central‑1 (Frankfurt)**. Transfers outside UK/EEA occur only:

- to sub‑processors with UK adequacy regulations; **or**
- under UK Addendum‑to‑SCCs or other lawful transfer mechanism.

8 Liability & Indemnity

Each Party's liability under this Agreement is subject to, and forms part of, the limitation‑of‑liability clause in the Master SaaS Agreement.

9 Governing Law & Jurisdiction

This Agreement is governed by the laws of England and Wales. The courts of London have exclusive jurisdiction.

Schedule 1 Technical & Organisational Measures

Area	Measures
Data in transit	TLS 1.3 enforced; HSTS; perfect‑forward secrecy.

Data at rest	AES-256 encryption; keys managed via AWS KMS; all records *hashed* (SHA-256) whenever verification accuracy permits.
Pseudonymisation	Email & phone stored as salted hashes where operationally feasible; raw values cached ≤ 24 h for lookup reconciliation.
Access control	Mandatory MFA on account creation; customers may enforce MFA on every login via policy flag.
Network security	VPC isolation; security-group least privilege; WAF with OWASP ruleset; inbound traffic restricted to HTTPS & SFTP.
Monitoring & logging	Centralised log aggregation (AWS CloudWatch); 30-day log retention; anomaly alerts (AWS GuardDuty).
Vulnerability management	Weekly dependency scanning; quarterly external penetration test; critical patches ≤ 72 h.
Business continuity	Multi-AZ deployment; automated snapshots; RPO ≤ 4 h, RTO ≤ 24 h.
Employee controls	Background checks; signed confidentiality agreements; security training on hire and annually.

Schedule 2 Approved Sub-processors

Sub-processor	Purpose	Location	Safeguards
Amazon Web Services EMEA SARL	Hosting, storage, networking	UK & Germany (eu-west-2, eu-central-1)	ISO 27001, SOC 2 Type II
UK Mobile Network Operators (BT, Vodafone, O2, EE)	HLR lookup for phone verification	United Kingdom	Traffic routed via secure API; no data persisted by MNOs
Email-verification provider (TBD, optional)	Supplementary mailbox validation	EEA	Added only on written request; SCCs in place
IP-fraud detection provider (TBD, optional)	Risk scoring	EEA/UK	Added only on written request; SCCs in place

Controller will be notified, with right to object, before any additional sub-processor is engaged.

Executed by the Parties:

For Horizon Landings Ltd (t/a Rivelin)

Name: ____________________________

Title: ____________________________

Date: ____________________________

For Customer

Name: ____________________________

Title: ____________________________

Date: ____________________________