Data Processing Agreement

Version 1.1 · Effective 28 August 2026 · Phone Validation and Current Carrier Lookup

This DPA is pre-signed and requires no signature from Veriphone. It applies automatically to every customer who accepts our Terms of Service, on every plan including the free one. You do not need to contact us, and you do not need an Enterprise Agreement, to rely on it.

Download the signed PDF — countersign it if your process requires, and file it. Nothing needs to come back to us.

Parties

Processor: Epic Grove Ltd, trading as Veriphone, a company registered in England & Wales (company number 17285617), 128 City Road, London, EC1V 2NX, United Kingdom ("Veriphone", "we").

Controller: the customer identified in the Agreement ("Customer", "you").

1. Background and scope

1.1 This Data Processing Agreement ("DPA") forms part of, and is subject to, the Veriphone Terms of Service or other written agreement between the Parties (the "Agreement"). Where this DPA conflicts with the Agreement on the subject of personal data processing, this DPA prevails.

1.2 This DPA applies where Veriphone processes Customer Personal Data on the Customer's behalf in providing the Services.

1.3 **Roles.** For Customer Personal Data, the Customer is the **controller** and Veriphone is the **processor**. Where Veriphone processes personal data of the Customer's own account administrators for account management, billing, security and service communications, Veriphone acts as an independent **controller** for that limited purpose, governed by its Privacy Policy and not by this DPA.

1.4 **Definitions.** "Data Protection Law" means the UK GDPR and the Data Protection Act 2018, and Regulation (EU) 2016/679 ("EU GDPR") together with its implementing laws, each to the extent applicable. "Customer Personal Data", "personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "supervisory authority" carry the meanings given in Data Protection Law. "Sub-processor" means a third party engaged by Veriphone to process Customer Personal Data.

1.5 **Services covered.** This DPA applies to all Services under which Veriphone processes Customer Personal Data on the Customer's behalf, namely:

- **Phone Validation** — the standard lookup: validation and enrichment, in which the submitted telephone number is processed entirely within Veriphone's own systems and reference datasets; and

- **Current Carrier Lookup** (requested with `mode=current`) — in which the submitted telephone number is additionally checked against a third-party number portability data source in order to identify the carrier currently serving that number.

Both are described in **Annex I**. The disclosure made in providing Current Carrier Lookup is governed by clause 5.5.

2. Processing on documented instructions

2.1 Veriphone shall process Customer Personal Data only on the Customer's documented instructions, including with regard to transfers to a third country, unless required to do so by law to which Veriphone is subject. In that case Veriphone shall inform the Customer of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

2.2 The Agreement, this DPA (including Annex I), and the Customer's use of the Services through their documented interfaces constitute the Customer's complete documented instructions.

2.3 Veriphone shall inform the Customer if, in its opinion, an instruction infringes Data Protection Law. Veriphone may suspend performance of the affected instruction pending resolution.

2.4 **Veriphone shall not** sell Customer Personal Data, use it for its own marketing, or use it to train machine-learning models. Veriphone may generate and use aggregated, non-identifying statistics about service usage (for example request volumes, latency, and country distribution), provided such statistics contain no personal data and cannot be attributed to any data subject.

3. Confidentiality

3.1 Veriphone shall ensure that persons authorised to process Customer Personal Data are bound by an appropriate duty of confidentiality, whether contractual or statutory.

3.2 Veriphone shall limit access to Customer Personal Data to personnel who require access to perform the Agreement.

4. Security

4.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk to data subjects, Veriphone shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in **Annex II**.

4.2 Veriphone may update the measures in Annex II provided the level of security is not materially reduced.

5. Sub-processors

5.1 The Customer grants Veriphone **general authorisation** to engage Sub-processors for the processing of Customer Personal Data. The Sub-processors engaged at the date of this DPA are listed in **Annex III** and on our security page.

5.2 Veriphone shall give the Customer at least **thirty (30) days'** prior notice of the addition or replacement of any Sub-processor, by updating the security page and notifying the Customer by email where the Customer has subscribed to such notifications.

5.3 The Customer may object to a change on reasonable data-protection grounds within the notice period. Where the Parties cannot resolve the objection, the Customer may terminate the affected Services on written notice, with a pro-rata refund of prepaid, unused fees.

5.4 Veriphone shall impose on each Sub-processor, by written contract, data protection obligations no less protective than those in this DPA, and **remains fully liable to the Customer** for the performance of that Sub-processor's obligations.

5.5 **Independent data sources.** In providing Current Carrier Lookup, Veriphone submits the queried telephone number to a third-party number portability data provider. That provider maintains its own reference dataset, determines the purposes and means of processing that dataset, and answers the query from it. It does not process Customer Personal Data on Veriphone's documented instructions. It is therefore an **independent controller in respect of its own dataset, and is not a Sub-processor**; clauses 5.1 to 5.4 do not apply to it.

5.6 The disclosure under clause 5.5 is limited to **the telephone number queried**. No Customer identity, account identifier, uploaded file, file content, result data or other Customer data is disclosed. The provider is located in the **United Kingdom** and is engaged by Veriphone under a written contract containing confidentiality and data protection obligations.

5.7 Veriphone may substitute or add number portability data providers at any time. The limits in clause 5.6 continue to apply to any such provider.

6. Data subject rights

6.1 Taking into account the nature of the processing, Veriphone shall assist the Customer by appropriate technical and organisational measures, insofar as reasonably possible, in fulfilling the Customer's obligation to respond to requests to exercise data subject rights under Chapter III of the GDPR.

6.2 Where Veriphone receives a request directly from a data subject relating to Customer Personal Data, Veriphone shall not respond to the substance of the request, and shall promptly forward it to the Customer.

6.3 Because Veriphone holds Customer Personal Data only as described in Annex I and does not maintain an independent index of data subjects, the Customer acknowledges that assistance under this clause is provided through the deletion, export and access functions of the Services, and by reasonable cooperation on request.

7. Personal data breach, DPIA and prior consultation

7.1 Veriphone shall notify the Customer **without undue delay, and in any event within seventy-two (72) hours**, after becoming aware of a personal data breach affecting Customer Personal Data.

7.2 The notification shall describe, to the extent known: the nature of the breach and the categories and approximate number of data subjects and records concerned; the likely consequences; the measures taken or proposed; and a contact point for further information. Where information is not available at the time of notification, it shall be provided in phases without undue delay.

7.3 Veriphone shall provide reasonable assistance to the Customer with data protection impact assessments and prior consultation with a supervisory authority under Articles 35 and 36 GDPR, taking into account the nature of processing and the information available to Veriphone.

8. Deletion and return

8.1 **Customer-initiated deletion.** The Customer may delete uploaded files and their outputs at any time through the Services. Deletion removes the underlying stored objects.

8.2 **Deletion of aged files.** Veriphone may delete uploaded files and their outputs more than **ninety (90) days** after upload. The Customer is responsible for downloading result files, and for deleting files it no longer requires, within that period. Veriphone does not guarantee deletion within any particular period during the term.

8.3 **Deletion on termination.** On expiry or termination of the Agreement, or on closure of the Customer's account, Veriphone shall, at the Customer's election, delete or return all Customer Personal Data and delete existing copies, within **thirty (30) days**, unless storage is required by law to which Veriphone is subject. Closure of the Customer's account through the Services deletes the Customer's stored files as part of that operation.

8.4 Retention periods applicable during the term of the Agreement are set out in **Annex I, section 6**.

9. Audit and information

9.1 Veriphone shall make available to the Customer all information reasonably necessary to demonstrate compliance with Article 28 GDPR.

9.2 Veriphone shall allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer. The Customer shall give at least thirty (30) days' written notice, audits shall occur no more than once in any twelve-month period (except following a

personal data breach or where required by a supervisory authority), shall be conducted during business hours, shall not unreasonably disrupt Veriphone's operations, and shall be subject to confidentiality obligations.

9.3 Veriphone may satisfy an audit request by providing its then-current security documentation and responding to a reasonable security questionnaire, where this addresses the Customer's requirements.

9.4 Veriphone does **not** currently hold SOC 2, ISO 27001 or equivalent third-party certification.

10. International transfers

10.1 Customer Personal Data is stored and processed in the **European Economic Area**, as set out in Annex I, section 5, save for the disclosure of a queried telephone number to a number portability data provider located in the United Kingdom, as described in clause 5.5.

10.2 Veriphone is established in the **United Kingdom**. Where processing under this DPA involves a transfer of Customer Personal Data outside the European Economic Area, the Parties agree that the transfer is made:

- in reliance on any adequacy decision then in force in respect of the United Kingdom; or
- failing that, subject to the Standard Contractual Clauses adopted by the European Commission (Decision 2021/914), Module Two (controller to processor), and/or the UK International Data Transfer Addendum, as applicable — incorporated by reference and completed as set out in Annex IV.

10.3 Veriphone shall not transfer Customer Personal Data outside the EEA or the United Kingdom other than as described in Annex I and Annex III.

11. Liability and term

11.1 Each Party's liability under this DPA is subject to the limitations and exclusions of liability set out in the Agreement.

11.2 This DPA takes effect on the date the Customer accepts the Agreement and continues for as long as Veriphone processes Customer Personal Data. Clauses 3, 8, 9, 10 and 11 survive termination.

11.3 This DPA is governed by the laws of England and Wales, and the courts of England and Wales have exclusive jurisdiction, save where Data Protection Law requires otherwise.

Annex I — Details of processing

1. Subject matter. Provision of phone number validation, enrichment and carrier lookup services via API, batch CSV upload, and integrations. Both kinds of lookup are covered: **Phone Validation** (the standard lookup) and **Current Carrier Lookup** (requested with `mode=current`).

2. Duration. The term of the Agreement, plus the retention periods in section 6.

3. Nature and purpose.

Phone Validation (standard lookup). Receiving phone numbers submitted by the Customer; validating their format and structure; enriching them with country, region, carrier and line-type attributes derived from Veriphone's own reference datasets; and returning the result to the Customer. For batch processing, reading an uploaded file, processing each row, and producing a result file. The submitted number does not leave Veriphone's systems.

Current Carrier Lookup (requested with `mode=current`). In addition to the above, submitting the queried telephone number to a third-party number portability data provider in order to identify the carrier currently serving that number, and returning that result to the Customer. **Only the telephone number itself is disclosed** — see clause 5.5. Veriphone does not receive or retain any additional personal data about the data subject from that provider; the response describes the number, not the person.

4. Categories of personal data.

- **API requests** — phone numbers submitted by the Customer.
- **Batch CSV uploads** — phone numbers, plus any other columns the Customer chooses to include in the uploaded file, which may include names or other identifiers.
- **Result files** — the above, plus the validation and enrichment attributes returned.

Veriphone does not require, and does not ask for, any category of data beyond a phone number. Additional columns present in an uploaded file are passed through unmodified and are processed only incidentally.

Categories of data subjects: the individuals to whom the submitted phone numbers relate, as determined by the Customer — typically the Customer's own customers, users, leads or contacts.

Special categories of data: none. The Customer shall not submit special category data under Article 9 GDPR or criminal offence data under Article 10 GDPR.

5. Processing locations. All processing takes place in the **European Economic Area**. Compute runs in Belgium; uploaded files, result files, job metadata and operational logs are held in EU multi-region storage spanning Belgium and the Netherlands.

In providing Current Carrier Lookup, the queried telephone number is disclosed to a third-party number portability data provider located in the **United Kingdom** — see clause 5.5 and clause 10.

6. Retention.

- **Phone numbers submitted to the API** — not persisted to any database. Processed in memory and returned in the response. Not written to application logs, and not present in usage analytics.
- **Operational request logs** — where the Customer calls the API using a `GET` request, the request URL, including the submitted phone number, is recorded in infrastructure request logs and retained for **30 days**, after which it is automatically deleted. Customers who prefer to avoid this may submit

parameters in a `POST` body.

- **Service usage statistics** — aggregate only: request counts, credit consumption, country distribution. Contains no phone numbers and no personal data. Retained for the term of the Agreement.
- **Numbers submitted for Current Carrier Lookup — not persisted to any database by Veriphone.** The number is disclosed to the number portability data provider for the purpose of answering the query (clause 5.5) and the result is returned in the response. Retention by that provider is determined by that provider as an independent controller.
- **Uploaded files and result files** — retained until the Customer deletes them through the Services. Veriphone **may** delete files and their outputs more than **90 days** after upload (clause 8.2); the Customer is responsible for downloading result files within that period. Veriphone does not guarantee deletion within any particular period during the term.
- **Job metadata** (filename, row counts, status, timestamps) — retained for the term of the Agreement. Contains no phone numbers.

On termination or account closure, all Customer Personal Data — including all stored files — is deleted in accordance with clause 8.3.

Annex II — Technical and organisational measures

Encryption. All data in transit is protected by TLS. All data at rest is encrypted using Google-managed encryption keys (AES-256).

Access control. Access to Customer Personal Data requires authentication with a Customer-specific API key. Administrative access to production infrastructure is restricted to authorised personnel through the cloud provider's identity and access management, and is limited to those who require it.

Segregation. Uploaded files are stored under a per-account path and are accessible only through authenticated, account-scoped endpoints.

Minimisation. Phone numbers submitted to the API are not written to any database. Usage analytics are aggregated and contain no personal data.

Resilience. Services run on Google Cloud managed infrastructure with provider-level redundancy and durability. Data is stored in multi-region EU storage.

Deletion. Customers can delete uploaded files and their outputs at any time via the Services; deletion removes the underlying stored objects. Closing an account deletes that account's stored files in the same operation. Files and their outputs are eligible for deletion more than 90 days after upload.

Vulnerability management. Dependencies are updated as part of the regular release process.

Certification. Veriphone does not currently hold SOC 2, ISO 27001 or equivalent third-party certification.

Annex III — Sub-processors

- **Google Cloud EMEA Limited** (Ireland) — compute, storage, database and logging infrastructure, located in the EEA as set out in Annex I section 5.

One sub-processor, for the whole service. This list is complete for *both* Phone Validation and Current Carrier Lookup. Sub-processors are legal entities, not products: Google Cloud's breadth means Veriphone's entire infrastructure sits behind that single entity, which is why one row covers all compute, storage, database and logging.

Not sub-processors. The third-party number portability data provider used for Current Carrier Lookup is an **independent controller** in respect of its own dataset and is not a sub-processor — see clause 5.5. Other third parties engaged by Veriphone in connection with your own account — payment processing, transactional email and customer relationship management — receive no Customer Personal Data and are not sub-processors for the purposes of this Annex. Veriphone is controller for that data, and the categories of recipient are disclosed in our Privacy Policy.

Changes to this list. Veriphone gives at least **thirty (30) days' prior notice** of the addition or replacement of any sub-processor, by updating our security page and by email where the Customer has subscribed to such notifications. The Customer may **object** on reasonable data-protection grounds within that period; where the objection cannot be resolved, the Customer may terminate the affected Services with a pro-rata refund of prepaid, unused fees. See clauses 5.2 and 5.3. To subscribe, email privacy@veriphone.io.

Annex IV — Standard Contractual Clauses

Where clause 10.2(b) applies, the Standard Contractual Clauses are incorporated by reference and completed as follows: the **data exporter** is the Customer; the **data importer** is Epic Grove Ltd; **Module Two** (controller to processor) applies; the optional docking clause is included; the **governing law and forum** are those stated in clause 11.3; **Annex I** to the Clauses is populated by Annex I above; **Annex II** to the Clauses is populated by Annex II above; and the list of sub-processors is Annex III above. Where the UK International Data Transfer Addendum applies, it is incorporated with the same annexes.

Signature

This DPA is incorporated into the Veriphone Terms of Service and applies automatically to every account. It is **signed in advance by Epic Grove Ltd**, so nothing is required from Veriphone, and no countersignature is required from the Customer for it to take effect (clause 11.2).

The Customer may countersign where its own procedures require a signed copy on file.

	Processor	Controller
Signed	*Adil Ben El Khattab*	

Name	Adil BEN EL KHATTAB	
Title	Director	
For and on behalf of	Epic Grove Ltd, company no. 17285617	
Date	28 August 2026	

Questions

For questions about this DPA, or to subscribe to sub-processor change notifications, email privacy@veriphone.io.

Wording note, 12 November 2026: the names of the two lookups in this document were aligned with the website ("standard lookup", "Current Carrier Lookup"). The terms of Version 1.1 are unchanged.

If your organisation requires a *negotiated* DPA rather than this published one, see Enterprise Agreement.