

Data Processing Agreement

Version 1.0 · Effective 26 October 2026 · simplecold.com/gdpr

This Data Processing Agreement (DPA) is between SimpleCold and the customer identified below (Customer). It forms part of the SimpleCold Terms of Service and applies automatically to Customer's use of the Service where Data Protection Law applies. A signature is needed only if Customer wants a countersigned copy: complete the signature block, sign and email it to privacy@simplecold.com, and SimpleCold will countersign and return it.

1 Definitions

In this DPA:

- **Data Protection Law** means the EU General Data Protection Regulation 2016/679 (GDPR), the GDPR as it forms part of UK law together with the UK Data Protection Act 2018 (UK GDPR), the Swiss Federal Act on Data Protection, and any other data protection law that applies to the processing of Customer Personal Data under the Agreement.
- **Agreement** means the SimpleCold Terms of Service (simplecold.com/terms) under which SimpleCold provides the Service to Customer.
- **Service** means the SimpleCold email verification service: the dashboard, the API and related features.
- **Customer Personal Data** means personal data that Customer, or its users, submit to the Service for verification, including uploaded files, addresses sent through the API and contacts imported from connected services, as described in Annex 1.
- **Subprocessor** means a third party engaged by SimpleCold that processes Customer Personal Data.
- **SCCs** means the standard contractual clauses approved by European Commission Implementing Decision (EU) 2021/914; **UK Addendum** means the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner.
- **Controller, processor, data subject, personal data, processing and personal data breach** have the meanings given in the GDPR.

2 Scope and roles

This DPA applies when SimpleCold processes Customer Personal Data in providing the Service. For Customer Personal Data, Customer is the controller (or a processor acting for its own controller) and SimpleCold is the processor. This DPA forms part of the Agreement.

SimpleCold is an independent controller of the personal data it needs to run its own business, such as account and billing data, security logs and the verification result cache described in section 11. That processing is covered by the SimpleCold Privacy Policy (simplecold.com/privacy), not by this DPA.

3 Customer's responsibilities

- Customer is responsible for having a lawful basis for the Customer Personal Data it submits and for any email it later sends to the people concerned.
- Customer will not submit special categories of personal data, data relating to criminal convictions, or data about children.
- Customer's instructions to SimpleCold will comply with Data Protection Law.

4 Processing on instructions

SimpleCold will process Customer Personal Data only on Customer's documented instructions, which are the Agreement, this DPA and Customer's use and configuration of the Service, unless the law requires otherwise; in that case SimpleCold will tell Customer before processing unless the law forbids it. SimpleCold will tell Customer if, in its opinion, an instruction breaks Data Protection Law.

5 Confidentiality

SimpleCold will ensure that everyone it authorises to process Customer Personal Data is bound by a duty of confidentiality and has access only as needed to provide and support the Service.

6 Security

SimpleCold will implement and maintain the technical and organisational measures described in Annex 2, appropriate to the risk of the processing. SimpleCold may update these measures as long as the overall level of protection is not reduced.

7 Subprocessors

1. Customer gives SimpleCold general authorisation to engage Subprocessors. The Subprocessors in use at the date of this DPA are listed in Annex 3 and at simplecold.com/subprocessors.
2. SimpleCold will notify Customer's account owner by email at least 14 days before adding or replacing a Subprocessor. Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, Customer may stop using the affected part of the Service and close its account.
3. SimpleCold will impose data protection obligations on each Subprocessor that are no less protective than this DPA, and remains responsible to Customer for its Subprocessors' performance of those obligations.

8 Data subject requests

Taking into account the nature of the processing, SimpleCold will help Customer, by appropriate measures and as far as possible, to respond to requests from data subjects to exercise their rights. If SimpleCold receives such a request directly about Customer Personal Data, it will refer the data subject to Customer and, where it can identify Customer, forward the request without undue delay.

9 Personal data breaches

SimpleCold will notify Customer without undue delay, and where feasible within 48 hours, after becoming aware of a personal data breach affecting Customer Personal Data. The notice will describe, as far as then 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. SimpleCold will provide further information as it becomes available and take reasonable steps to contain the breach.

10 Impact assessments and consultation

SimpleCold will give Customer reasonable assistance, using information available to it, with data protection impact assessments and prior consultations with supervisory authorities that relate to the Service.

11 Verification result cache

To provide accurate results efficiently and to limit requests to mail servers, SimpleCold keeps a record of the verification result for each address it checks: the address, its domain, category, reason, failure type, mail server and website country, website language and typo suggestion. This record contains no identifier of Customer, no reference to the source list or file and no other data from Customer's files. SimpleCold may use it to answer a later check of the same address for any customer within a limited reuse period (currently up to 30 days for a confirmed mailbox, 14 days for a risky result and 60 days for an undeliverable result; unconfirmed results are not reused).

SimpleCold processes this record as an independent controller under its Privacy Policy. On request, SimpleCold will delete specific addresses from it within 30 days.

12 Deletion and return

1. During the term of the Agreement, Customer can download the results of its verification jobs from the Service.
2. SimpleCold does not currently delete Customer Personal Data automatically. On Customer's written request to privacy@simplecold.com, and in any case after the Agreement ends and Customer asks for it, SimpleCold will delete Customer Personal Data (uploaded files, results files and job records) within 30 days, unless the law requires SimpleCold to keep it.
3. Copies held in routine system logs or backups are deleted as those logs and backups expire, and are protected under this DPA until then.

13 Information and audits

SimpleCold will make available to Customer the information reasonably necessary to demonstrate compliance with this DPA, including written answers to reasonable security questionnaires. If that information is not enough to demonstrate compliance, or a supervisory authority requires it, Customer may audit SimpleCold's compliance, no more than once a year, on at least 30 days' written notice, during business hours, at Customer's cost, by Customer or an independent auditor bound by confidentiality, and in a way that does not disrupt the Service or expose other customers' data.

14 International transfers

1. SimpleCold and its main Subprocessors process data in the United States. Where Customer Personal Data is transferred from the European Economic Area to SimpleCold in a country without an adequacy decision, the SCCs, Module Two (controller to processor), are incorporated into this DPA, with Customer as data exporter and SimpleCold as data importer. Where Customer is itself a processor, Module Three (processor to processor) applies instead.
2. For the SCCs: Clause 7 (docking clause) applies; under Clause 9 option 2 (general written authorisation) applies, with the notice period in section 7 of this DPA; the optional wording in Clause 11 does not apply; under Clause 17 option 1 applies and the SCCs are governed by the law of Ireland; under Clause 18 disputes are resolved by the courts of Ireland; Annex I is completed by Annex 1 of this DPA, Annex II by Annex 2 and Annex III by Annex 3. The competent supervisory authority is the one determined under Clause 13.
3. For transfers from the United Kingdom, the UK Addendum applies, completed with the information in this DPA; either party may end it only as the UK Addendum allows. For transfers from Switzerland, the SCCs apply with the references to the GDPR read as references to the Swiss Federal Act on Data Protection, and the Swiss Federal Data Protection and Information Commissioner is a competent supervisory authority.
4. Where a recipient is covered by an adequacy decision, such as certification under the EU-US Data Privacy Framework, SimpleCold may rely on that decision instead. If the SCCs conflict with this DPA, the SCCs prevail.

15 Liability

Each party's liability under this DPA is subject to the limitations of liability in the Agreement, to the extent Data Protection Law allows. Nothing in this DPA limits a data subject's rights under the SCCs.

16 Term and precedence

This DPA applies for as long as SimpleCold processes Customer Personal Data. If this DPA conflicts with the Agreement about the processing of Customer Personal Data, this DPA prevails. SimpleCold may update this DPA to reflect changes in law or in the Service, without reducing the protection it gives Customer, and will publish the current version at simplecold.com/gdpr.

Signatures

Customer

Company name

Address

Name

Title

Email

Date

Signature

SimpleCold

Name

Title

Email: privacy@simplecold.com

Date

Signature

A1 Annex 1: Details of processing

	Details
Data exporter	Customer, as identified in the signature block. Activities: verifying email addresses it holds before contacting them or storing them.
Data importer	SimpleCold, provider of the Service. Contact: privacy@simplecold.com . Activities: email verification.
Data subjects	People whose email addresses are in the lists, files and requests Customer submits to the Service, and in contacts Customer imports from connected services.
Categories of personal data	Email addresses; any other columns in files Customer uploads (for example names, job titles, company names); for HubSpot imports, contact ID, email, first name and last name.
Sensitive data	None. Customer must not submit special categories of data.
Frequency	Continuous, whenever Customer uses the Service.
Nature of processing	Collection, storage, structuring, retrieval and analysis: syntax checks, domain and mail server (DNS) lookups, throwaway and role address checks, catch-all detection, a mailbox-level check with the mail server, and producing results files.
Purpose	Providing the Service to Customer: telling Customer whether each address can receive email and why.
Retention	For the term of the Agreement until Customer asks for deletion; deletion within 30 days of the request (section 12).
Subprocessor transfers	As listed in Annex 3, for the purposes and data shown there, for the duration of the Agreement.

A2 Annex 2: Technical and organisational measures

- **Access control.** Passwordless sign-in with one-time email codes that expire after 10 minutes, or Google sign-in limited to verified Google email addresses with a one-time state check. Sessions are signed tokens in HTTP-only, Secure cookies that expire after 12 hours.
- **API keys.** Stored only as SHA-256 hashes with a short hint; optional expiry; can be deactivated or regenerated at any time; checked on every request; verification endpoints are rate-limited.
- **Encryption.** HTTPS for all traffic to the website, dashboard and API; TLS between application servers and the database and cache; encryption at rest provided by the database and storage providers.
- **Separation.** Files are stored under per-organisation paths, and jobs, files, results and API keys are returned only to members of the owning organisation or its API keys.
- **Storage.** Uploaded and results files are private objects; downloads use signed links that expire after a few minutes. Results files escape spreadsheet formulas.
- **Payments.** Card data is handled only by Stripe Checkout; Stripe webhooks are verified by signature.

- **Abuse prevention.** Per-IP limits and a bot check (Cloudflare Turnstile) on free tools; sign-ups from known throwaway domains are refused.
- **Personnel.** Production access is limited to the people who run the Service, who are bound by confidentiality, and administrative tools are behind separate authentication.
- **Schema and change safety.** Database changes are made only through versioned migrations; automatic schema synchronisation is disabled.
- **Incident handling.** Security reports to security@simplecold.com; breach notification under section 9.

A3 Annex 3: Subprocessors

Current at the effective date. The live list is at simplecold.com/subprocessors.

Subprocessor	Purpose	Personal data	Location
DigitalOcean	Application hosting, file storage, cache and application logs	All service data, including uploaded files, verification results and logs	United States (file storage in New York)
Neon	Primary database	Accounts, organisations, billing records, verification results	United States (AWS us-east-2, Ohio)
Resend	Service email (sign-in codes, invitations, job and credit notices)	Recipient name and email address, message content	United States
SMTP2GO	Backup email delivery, used only if the main provider is unavailable	Recipient name and email address, message content	On request from privacy@simplecold.com