Data Processing Addendum

Beacon. Last updated 18 October 2026.

DRAFT: this document has not yet been reviewed by a lawyer and may change before it takes effect.

1. Parties

Party	Details
Controller (the "Customer")	The organisation that holds the account, as named in the account or order.
Processor	To be confirmed by the operator before signature
Processor registered address	To be confirmed by the operator before signature
Processor company number	To be confirmed by the operator before signature
Processor ICO registration	To be confirmed by the operator before signature
Processor privacy contact (and DPO, if appointed)	privacy@terapixel.co.uk

This addendum takes effect when the Customer accepts the Terms of Service or signs an order that refers to it, and applies from the date the Processor first processes Customer Personal Data.

2. Scope and definitions

This Data Processing Addendum ("DPA") is part of the agreement between you ("Customer") and Terapixel ("we", "Processor") under our Terms of Service (https://beaconmail.co/terms). It applies to the extent that we process Customer Personal Data on your behalf when you use the service, and is intended to meet Article 28 of the UK GDPR and the EU GDPR (together, "Data Protection Law").

Terms such as "controller", "processor", "personal data", "processing", "data subject", "personal data breach" and "supervisory authority" have the meanings given in Data Protection Law. "Customer Personal Data" means the personal data in Your Data (such as subscriber and contact records, and engagement data) that we process on your behalf. "Sub-processor" means a third party we engage to process Customer Personal Data.

3. Roles and instructions

For Customer Personal Data, you are the controller (or a processor acting for your own controller) and we are the processor. You are responsible for the lawfulness of the processing, including having a valid lawful basis and the consents that are required to email your contacts, and for giving them the information the law requires.

We will process Customer Personal Data only on your documented instructions, which are: the agreement, your use and configuration of the service, and any further written instructions you give that are consistent with the agreement. If we believe an instruction breaks Data Protection Law we will tell you, and we may suspend the instruction until it is resolved. Details of the processing are in Annex 1.

We act as an independent controller for the personal data of your users that we need to run your account, as set out in our Privacy Policy (https://beaconmail.co/privacy).

4. Confidentiality

We make sure that people authorised to process Customer Personal Data are bound by a duty of confidentiality and receive appropriate data protection training, and we limit access to those who need it to provide the service.

5. Security

We implement technical and organisational measures appropriate to the risk, as described in Annex 2. We may update them from time to time, provided that the overall level of protection is not reduced.

6. Sub-processors

You give us general authorisation to engage Sub-processors, including those on our sub-processors page (https://beaconmail.co/sub-processors). We will bind each Sub-processor to data protection obligations that are no less protective than those in this DPA, and we remain responsible for their performance.

We will give you at least 30 days' notice of the addition or replacement of a Sub-processor, by updating that page and publishing a dated change notice on it, which is also available as a feed (https://beaconmail.co/sub-processors/feed.xml). You may object on reasonable data protection grounds within that period. If we cannot reasonably accommodate your objection, you may end the affected service and receive a pro-rata refund of any prepaid fees for the period after termination.

Providers that you connect yourself (for example your own email sending provider, DNS provider or AI account) are chosen by you. They act as your processors, and we use them only to carry out your instructions.

7. Assisting with data subject requests

Taking into account the nature of the processing, we will help you respond to requests from data subjects who exercise their rights, mostly through features of the service such as search, export, edit and delete, and unsubscribe and suppression handling. If a data subject contacts us directly about Customer Personal Data, we will redirect them to you and not respond except as instructed or required by law.

8. Personal data breaches

We will notify you without undue delay after becoming aware of a personal data breach affecting Customer Personal Data, and give you the information we have that you reasonably need to meet your own notification duties, including the nature of the breach, the likely consequences, and the measures taken or proposed. We will take reasonable steps to contain and remediate the breach.

9. Impact assessments and prior consultation

We will give you reasonable help with data protection impact assessments and consultations with supervisory authorities that relate to our processing, taking into account the nature of the service and the information available to us.

10. Return and deletion

During the term you can export Customer Personal Data at any time from the dashboard. After the agreement ends we will make it available for export for a reasonable period and then delete it, including existing copies, unless the law requires us to keep it. Copies in routine backups are deleted as the backups are overwritten. You may ask us to delete it sooner.

11. Information and audits

We will make available the information reasonably necessary to show that we comply with this DPA, such as answers to security questionnaires and summaries of our practices. If that is not enough to satisfy Data Protection Law or a regulator, you may, on reasonable notice and no more than once a year (unless a breach or a regulator requires otherwise), carry out an audit, subject to confidentiality, during normal business hours, without disrupting the service or other customers, and at your cost.

12. International transfers

We will not transfer Customer Personal Data outside the UK or the European Economic Area unless an appropriate safeguard is in place. Where a transfer is to a country without an adequacy decision, the parties agree that the EU

Standard Contractual Clauses (Module Two: controller to processor, and Module Three where you are a processor) apply, as supplemented for UK transfers by the ICO's International Data Transfer Addendum, and that they are incorporated into this DPA by reference. The details required to complete them are in Annex 1, Annex 2 and Annex 3 and on the sub-processors page (https://beaconmail.co/sub-processors).

13. Liability, term and precedence

Each party's liability under this DPA is subject to the limits and exclusions in the Terms of Service. This DPA lasts for as long as we process Customer Personal Data. If there is a conflict between this DPA and the Terms of Service about the processing of personal data, this DPA prevails. The governing law and courts are those in the Terms of Service, except where the Standard Contractual Clauses require otherwise.

14. Annex 1: Details of the processing

Item	Detail
Subject matter	Provision of the Beacon email marketing service to the Customer.
Duration	For the term of the agreement, and the period after it described under "Return and deletion".
Nature of processing	Hosting, storing, organising, segmenting, transmitting by email, measuring engagement with, and deleting contact data.
Purpose	To enable the Customer to design, send, automate and measure email communications and manage its audience, and to provide support and keep the service secure.
Types of personal data	Email addresses, names, and other fields the Customer chooses to store (for example company, location, tags and preferences); consent and unsubscribe status; engagement data such as opens, clicks, bounces and complaints, with associated IP address and device or client information; form and survey responses the Customer collects.
Special categories	None intended. The Customer must not upload special category or criminal-offence data unless it has a lawful basis and has told us in advance.
Data subjects	The Customer's subscribers, contacts, leads, customers and survey respondents; and the Customer's own users to the extent they appear in Customer content.
Frequency	Continuous, for the duration of the service.
Transfers	To Sub-processors listed on the sub-processors page, under the safeguards described in the "International transfers" section.

15. Annex 2: Security measures

- **Access control.** Role-based access with least privilege; separate customer organisations; strong authentication and login protection with rate limiting; access to production data limited to authorised staff.
- **Encryption.** Encryption in transit over TLS; credentials and API secrets encrypted at rest with authenticated encryption.
- **Logging.** Audit logging of administrative and sensitive actions, and security event monitoring.
- **Resilience.** Regular backups, and processes to restore availability and access to data in a timely way after an incident.
- **Secure development.** Dependency management and review of changes before release; separation of environments; secrets kept out of source code.
- **Sending safeguards.** Sending-domain verification, mandatory unsubscribe handling, and suppression of bounced and complaining addresses.
- **Organisational.** Confidentiality obligations, security awareness, vendor due diligence for Sub-processors, and an incident response process.
- **Deletion.** Secure deletion of data on request and when the agreement ends, as described above.

16. Annex 3: International transfer details

This Annex records the choices needed to complete the transfer safeguards in the "International transfers" section. It is a draft: the entries marked for counsel must be decided by the operator's legal adviser before this addendum is relied on.

Item	Entry
EU Standard Contractual Clauses	Module Two (controller to processor), and Module Three (processor to processor) where the Customer is itself a processor.
Clause 7 (docking clause)	To be decided by counsel.
Clause 9(a) (sub-processors)	General written authorisation, with the notice period in the "Sub-processors" section.
Clause 11(a) (optional redress body)	To be decided by counsel.
Clause 13 (supervisory authority)	To be decided by counsel for the EU; the Information Commissioner's Office for UK transfers.
Clauses 17 and 18 (governing law and courts)	The law and courts of an EU Member State, to be chosen by counsel.
UK International Data Transfer Addendum	Table 1 (parties) as in the "Parties" section; Table 2 (selected SCCs) as above; Table 3 (appendix information) as Annex 1, Annex 2 and the sub-processors page; Table 4 (ending the addendum): to be decided by counsel.
UK International Data Transfer Agreement (IDTA)	May be used instead of the UK Addendum where the parties prefer it. To be decided by counsel.
Transfer risk assessment	To be carried out by the operator for each country outside the UK and the EEA that receives Customer Personal Data, using the locations on the sub-processors page.