Footer365

Data Processing Terms v2026-10-12

Document	Data Processing Terms
Version	v2026-10-12
Published	12 October 2026
Status	Published
Address	footer365.com/dpa

Documents

Document	Version	SHA-256 fingerprint
Data Processing Terms	v2026-10-12	`2df4 262f d596 dd51 692a 9565 6691 4545 260d 8624 16d4 8ab1 5fc4 86b7 4daf a3b6`

Each fingerprint is the SHA-256 of the document's exact text as published. Anyone can check that a saved copy matches the published version, and any change to the text would change its fingerprint. The current version of each document is published at footer365.com, and every version that applied to the organisation is kept on the Agreements page of its Footer365 portal.

Data Processing Terms

Data Processing Terms v2026-10-12, in force from 12 October 2026

SHA-256 fingerprint: 2df4 262f d596 dd51 692a 9565 6691 4545 260d 8624 16d4 8ab1 5fc4 86b7 4daf a3b6

Legal

Data Processing Terms

In force from 12 October 2026

1. Scope

1.1 These terms form part of the Footer365 Customer Agreement between Chillishot Limited, trading as Footer365 ("Footer365", "we"), and the customer ("Customer", "you"). They apply when we process personal data on your behalf in providing the service.

1.2 You are the controller and we are your processor for the processing described in the Annex. We are a controller of the personal data we use to run our relationship with you, as described in our privacy policy; these terms do not apply to that.

1.3 "Data Protection Law" means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and, where they apply to the processing, the EU GDPR and other data protection laws. Terms such as "controller", "processor", "personal data", "personal data breach" and "data subject" have the meanings given in the UK GDPR.

2. Your instructions

2.1 We process personal data only on your documented instructions, including about transfers outside the UK, unless the law requires otherwise, in which case we will tell you before processing unless the law forbids it.

2.2 Your instructions are this agreement, the settings you choose in the service, and any other written instruction you give that is consistent with it. They include our creating anonymous, aggregated information that does not identify you or any person, as section 12.4 of the Customer Agreement describes. Actions your managing reseller takes in your portal are treated as your instructions to us. We will tell you if we believe an instruction breaks Data Protection Law.

2.3 You are responsible for having a lawful basis for the processing, for the accuracy of the data, and for giving the people concerned the information the law requires about it, including your staff whose details appear in signatures and the recipients of messages carrying campaign banners.

3. Our people

Everyone we authorise to process the personal data is bound by a duty of confidentiality and receives training appropriate to their role.

4. Security

4.1 We maintain appropriate technical and organisational measures to protect the personal data, as described in our Security description, taking account of the state of the art, the cost, and the nature, scope, context and purposes of the processing and the risks to people. They include:

- encryption of data in transit, and encryption at rest of the access tokens and credentials we hold for your organisation and for the services we connect to on its behalf;
- access to the servers, and to the credentials Footer365 uses to run the service, limited to the people who operate it;
- access to the service's administration limited to authorised staff with a business need, in line with our access management policy;
- separation of each customer's data at the application and database level;
- an audit log of actions taken in the service;

- handling message bodies only in memory while a signature is added, without writing them to disk.

4.2 We may change these measures, provided the overall level of security is not reduced.

5. Sub-processors

5.1 You authorise us to use the sub-processors listed on our website at /subprocessors.

5.2 We will tell you at least 30 days before adding or replacing a sub-processor, by email to your account owner and accounts contact and by updating the list. You may object on reasonable data protection grounds within that period. If we cannot reasonably accommodate the objection, you may end the affected Subscription, without any fee for the rest of a committed term, and receive a refund of fees paid in advance for the period after it ends.

5.3 We impose on each sub-processor, by a written contract, the same data protection obligations as these terms, as Article 28(4) of the UK GDPR requires, and remain responsible to you for its performance.

6. Transfers

We will not transfer the personal data outside the UK, or allow a sub-processor to do so, unless the transfer is to a country covered by UK adequacy regulations or is protected by the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or the UK-US Data Bridge, with any assessment the law requires.

Where the EU GDPR applies to your transfer of personal data to us, the transfer relies on the European Commission's adequacy decision for the United Kingdom. If that decision ceases to apply, we will agree with you the EU Standard Contractual Clauses or another mechanism EU law recognises, and until then will continue to protect the data as these terms require.

7. Helping you

Taking into account the nature of the processing and the information available to us, we will help you, by appropriate technical and organisational measures where possible:

- to respond to requests from people exercising their rights; we will pass on to you any request we receive directly, without responding to it ourselves unless you ask us to;
- to meet your obligations on security, personal data breaches, data protection impact assessments and prior consultation with a regulator.

We may charge a reasonable fee for help beyond what the service provides, unless the help is needed because of our breach.

8. Personal data breaches

We will notify you without undue delay after becoming aware of a personal data breach affecting your personal data. The notice will describe, as far as then known, the nature of the breach, the categories and approximate number of people and records concerned, the likely consequences, and the measures taken or proposed, so that you can meet your own obligations, including any report to a regulator; where not everything is known at once, we will give you the information in stages as it becomes available. We will not tell a regulator or the people affected about a breach of your personal data without your agreement, unless the law requires us to.

9. Deletion at the end

9.1 When the agreement ends, and once the 30 days in 9.2 have passed, we delete the personal data we process for you, including the directory data, the email processing log, click records and uploaded files, within a further 30 days, unless the law requires us to keep it.

9.2 At your choice, we will return the personal data to you before deleting it. You may export what the portal allows until 30 days after the agreement ends, and, on a request made within that period, we will send you a copy of the personal data we hold for you in the service, as files in a commonly used format, within 30 days of the request, at no charge.

9.3 Records in our audit log, which may include the names and email addresses of the people who acted in the service, are not deleted under 9.1. After the agreement ends we keep them as a controller, to meet our legal obligations and to establish or defend legal claims, for the periods in our data retention policy, and then delete them.

10. Audits

We will make available the information reasonably necessary to show compliance with these terms, and allow audits by you or an auditor you appoint, who is bound by confidentiality and is not a competitor of ours, on 30 days' notice, during business hours, no more than once a year unless a regulator requires it or after a personal data breach. You pay the cost of the audit, unless it shows that we are in material breach of these terms, in which case we pay our own costs and reimburse your reasonable costs. We may meet a request by providing a recent independent report or certification where it covers the matter.

11. Liability

Each party's liability under these terms is subject to the limits in section 14 of the Customer Agreement, except where the law does not allow them to apply. Nothing in these terms limits either party's liability to a data subject under Article 82 of the UK GDPR.

Annex: details of the processing

Subject matter	Adding email signatures, disclaimers and banners to the customer's email, and running its signature campaigns
Duration	The term of the agreement, then until deletion under section 9
Nature of processing	Reading the customer's directory from Microsoft 365 and storing it; processing outbound email in transit to add a signature; recording information about each message processed; recording clicks on campaign links; hosting files the customer uploads
Purpose	To provide the service to the customer as described in the Customer Agreement

Data subjects: the customer's staff and other people in its Microsoft 365 directory; the senders of its email; the recipients of its email, whose email addresses Footer365 does not save, store or harvest; people who click links in its signatures and banners.

Categories of personal data:

- **Directory data**, synced from Microsoft 365 and stored: names, email addresses and aliases, job title, department, company name, business and mobile telephone numbers, office location, postal address, profile photograph, social media profile addresses, custom fields and Exchange extension attributes the customer chooses to use, group memberships, and any values the customer types in for its users.
- **Message data:**
    - processed in transit: the content of each outbound message, held in memory only while the signature is added and never written to disk; where the customer has turned on Bcc signature matching, a copy of an internal message may be held in memory for up to 30 seconds;
    - recorded: the sender's email address, the IP address of the sending mail server, the message identifier, the number of recipients, and which rule, template and campaign applied. Footer365 does not save, store or harvest recipients' email addresses. So that the relay can recognise Exchange delivering the same copy of a message twice, it keeps a one-way fingerprint of each copy's recipients, mixed with that message's identifier, from which no address can be read back; because it is derived from recipients' addresses, Footer365 treats the fingerprint as pseudonymised personal data and protects it in the same way as the rest of the record. For messages carrying a campaign banner, the domains of external recipients are recorded, up to 50 per message. No subject, recipient address or message body is stored.
- **Click data:** the time of a click on a tracked link, which link it was, the IP address and browser details of the device used, the type of email client and device, and whether the click appears to come from an automated link scanner. The IP address and browser details are deleted after 90 days, unless the customer sets another

period between 1 and 365 days; the rest of the click is kept for the campaign's statistics, and once those details are deleted it no longer identifies the person who clicked.

- **Files:** logos, images and photographs the customer uploads, which are publicly reachable by their address so they can be shown in email.
- **Add-in data:** when the Outlook add-in is used, the user's name and email address from Microsoft sign-in, and the domains of a message's recipients. The add-in does not read the message body, subject or attachments.

Special category data: none is intended. The customer must not put special category data into signatures.

Where it is processed: on Footer365's servers in the United Kingdom, hosted by LCN (Team Blue): the database, uploaded files, and the mail relay, whose only region today is the UK. Sub-processors and their locations are listed at /subprocessors.

Click records: Footer365 processes click records as the customer's processor, only to report campaign results to the customer. Footer365 is a controller only for its own use of the IP address of a request to protect the click tracking service from abuse, as its privacy policy describes.