Heatherstack

Data Processing Addendum

Last updated 19 November 2026

This Addendum forms part of our agreement with you. It applies whenever Heatherstack Limited processes personal data on your behalf, which mostly means data held in websites we host, maintain or build for you. It follows Article 28 of the UK GDPR.

1. Roles and law

1.1 You're the **controller**: you decide why and how your website collects personal data. We're the **processor**: we handle that data only to provide our services to you.

1.2 "**Data Protection Law**" means the UK GDPR, the Data Protection Act 2018, and any other data protection law that applies to the processing.

2. What we process

Subject matter	Hosting, maintaining, backing up, supporting and developing your website(s)
Duration	The length of our agreement, plus the deletion period in section 10
Nature and purpose	Storing, backing up, restoring and transmitting your website data, and viewing or editing it when needed to update, support or develop your site. We do this only to provide our services
Types of personal data	Whatever your website collects. Typically names, email addresses, phone numbers, postal addresses, form submissions, order and account details, IP addresses and server logs
Data subjects	Your website's visitors, customers, members and users, and your staff
Special category data	Not expected. Tell us before your site starts collecting health, biometric or other special category data, or criminal offence data, so we can agree any extra safeguards

3. Your responsibilities

3.1 You're responsible for having a lawful basis for the processing and a privacy notice on your website, and for getting consent for cookies where it's needed.

3.2 You choose the third-party services your site uses, such as analytics, tag managers, payment gateways and email marketing, and you hold your own agreements with them. They aren't our sub-processors unless they're listed in Annex A.

4. What we'll do

We'll:

1. process personal data only on your documented instructions, which are this agreement plus requests you make through our portal or by email, unless the law requires otherwise (in which case we'll tell you, unless the law prevents it);
2. tell you if we think an instruction breaks Data Protection Law;
3. make sure anyone we authorise to process the data is bound by confidentiality;
4. keep the data secure (section 5);
5. use sub-processors only as set out in section 6;
6. help you respond to people exercising their data protection rights (section 7);
7. help you meet your obligations on security, breach notification, data protection impact assessments and consultation with the ICO, as far as the nature of our processing allows;
8. delete or return the data when our agreement ends (section 10);
9. give you the information you reasonably need to show we're meeting these obligations (section 8).

5. Security

5.1 We take measures appropriate to the risk. Currently they include:

- hosting in UK data centres, whose physical security is managed by our hosting provider;
- each website in its own isolated hosting account;
- encrypted connections (HTTPS) for websites and admin areas, and key-based access to servers;
- two-factor authentication on our administrative accounts wherever the service supports it;
- a firewall, malware and vulnerability scanning, and prompt software updates;
- regular backups, with copies stored separately from the live server;
- access limited to Heatherstack personnel who need it, all bound by confidentiality.

5.2 We may change these measures as technology and risks change, but never in a way that lowers the overall level of protection.

6. Sub-processors

6.1 You authorise us to use the sub-processors listed in Annex A.

6.2 We'll give you at least 30 days' notice by email before adding or replacing a sub-processor. You can object on reasonable data protection grounds. If we can't resolve your objection, you can end the affected service without penalty, and we'll refund any unused prepaid fees.

6.3 Each sub-processor is bound by data protection terms that meet the requirements of Article 28. We remain responsible to you for their work.

6.4 Our sub-processors use sub-processors of their own. We'll send you our hosting provider's sub-processor list on request. When a sub-processor tells us about a change to its own sub-processors that affects your data, we'll forward it to you within 2 working days. If you object on reasonable data protection grounds, tell us within 10 days so we can raise it with them. If the change goes ahead anyway, you can end the affected service without penalty, and we'll refund any unused prepaid fees.

7. Individuals' rights

If someone contacts us to exercise their data protection rights about your website data, we'll pass the request to you promptly and won't respond ourselves unless you ask us to. We'll give you reasonable help to respond. If a request needs significant work, we may charge our hourly rate, and we'll tell you before we start.

8. Information and audits

We'll answer your reasonable questions and questionnaires about how we protect your data. If you or a regulator need to go further, we'll cooperate. That applies with reasonable notice, at your cost, no more than once a year unless a regulator requires it, and subject to confidentiality.

9. Personal data breaches

If we become aware of a personal data breach affecting your data, we'll tell you without undue delay. We aim to do so within 48 hours. We'll share what we know at the time and update you as we learn more. We'll also help you notify the ICO and affected individuals where you need to. The UK GDPR gives you 72 hours to notify the ICO.

10. When our agreement ends

10.1 You can have your data back as a full copy of your website (Schedule A, A10.1). We then delete it from our live systems within 30 days.

10.2 Backup copies are deleted automatically as they reach the end of their retention period.

10.3 We keep data for longer only if the law requires us to.

11. Transfers outside the UK

11.1 Your website is hosted in the UK. Some sub-processors in Annex A process data in other countries. Where a country isn't covered by UK adequacy regulations, the transfer is protected by the sub-processor's own UK transfer safeguards. These are the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses.

11.2 If you instruct us to host your website or data in a particular location outside the UK, that's your instruction as controller. We'll cooperate in putting any required transfer safeguards in place.

12. Liability and priority

12.1 The liability limits in our General Terms apply to this Addendum, except where the law doesn't allow them to.

12.2 If this Addendum conflicts with anything else in our agreement on data protection, this Addendum takes priority.

Annex A: Sub-processors

Sub-processor	What they do	Where data is processed
Kualo Limited	Hosting servers, on-server backups, and security and malware scanning	UK (London)
Cloudflare, Inc.	DNS, content delivery and security (website traffic passes through its network)	Global network; US company. Transfers covered by Cloudflare's own data processing terms.
Microsoft (OneDrive)	Offsite backup storage	UK
WP Umbrella	Additional backups and monitoring (some plans)	France
Hetzner Online GmbH	Staging, testing and supporting services	Germany

Last updated 19 November 2026.