Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the agreement between ThenMedia Limited and every customer who uses the website design, hosting, content management, email, digital signage and related services we provide under the Chrestos brand ("you" or "the Customer"). It is written for every kind of organisation we work with, including parish and town councils, businesses, charities, community groups, churches and schools, and it sets out the terms required by Article 28 of the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018.

By accepting our terms of service you agree to this DPA. No separate signature is needed. It applies alongside our Fair Usage Policy, Privacy Policy and Data Protection Policy.

1. Parties and Responsibilities

Data Processor: ThenMedia Limited, Charter Court, 2 Well House Barns, Chester Road, Bretton, Chester CH4 0DH. Company No. 07990449. VAT No. 132 3260 57. ICO Registration No. ZA362902. Chrestos is a trading name of ThenMedia Limited. In this DPA "we", "us" and "our" mean ThenMedia Limited.

Data Controller: the Customer, being the council, business, organisation or person named on the order or account for the services.

As Data Controller you decide why and how personal data is collected through your website and services. You are responsible for having a lawful basis for that processing, for giving privacy information to the people whose data you collect, and for approving the retention periods in Section 6.

As Data Processor we process personal data only on your documented instructions, in line with this DPA and our own legal obligations. We are a controller in our own right only for the limited data we need to run our business relationship with you, such as account contacts and billing details, and that data is covered by our Privacy Policy.

2. Scope of Data Processing

Subject matter: hosting, maintaining and supporting your website and content management system (the Cloud), together with any optional services you choose to use, such as online forms, bookings, an online shop, email and newsletters, members areas, social media publishing and digital signs.

Duration: for as long as we provide services to you, and afterwards until the data is deleted or returned under Section 7.

Nature and purpose: storing, hosting, backing up, transmitting, displaying and securing personal data so your services work, and, where you ask us to, adding or editing content and providing technical support.

Categories of individuals: your website visitors, residents, customers, members, parishioners, parents and pupils, volunteers, staff, councillors and trustees, website administrators, and anyone who contacts you or submits information through your website.

Types of personal data: names, email addresses, telephone numbers and postal addresses; the content of messages and form submissions; booking and order details; account details for administrators and members; images and documents you upload; and technical data such as IP addresses and browser information in server and security logs. Payment card details are handled directly by the payment provider and are never stored by us.

Sensitive data and children: some organisations, such as churches and schools, may hold data that reveals religious belief or relates to children. If you choose to collect or publish this kind of data through your website, you must make sure you have an appropriate lawful basis and condition for doing so and collect only what you need. Please tell us, so we can advise on suitable settings such as restricted access areas.

3. Data Protection Obligations

In line with Article 28 of the UK GDPR, ThenMedia Limited will:

• Process personal data only on your documented instructions (this DPA, our terms of service, and instructions you give through the Cloud or in writing), including in relation to any transfer outside the UK, unless the law requires otherwise. In that case we will tell you before processing unless the law prevents us.
• Make sure everyone authorised to process your data is bound by a duty of confidentiality.
• Apply the technical and organisational security measures in Section 4.
• Use sub-processors only as set out in Section 5.
• Help you respond to requests from individuals exercising their data protection rights.
• Help you meet your obligations on security, personal data breaches, data protection impact assessments and any prior consultation with the Information Commissioner's Office (ICO).
• Delete or return personal data at the end of the services, as set out in Section 7, unless the law requires us to keep it.
• Make available the information you need to show that these obligations are being met, and allow for and contribute to audits as set out below.
• Tell you straight away if we believe an instruction from you breaks data protection law.

Compliance information and audits

ThenMedia Limited holds Cyber Essentials certification, independently assessed every year. On request we will provide a copy of our current certificate and written answers to reasonable data protection questionnaires. We do not routinely permit third party audits of our systems, because our infrastructure is shared by many customers. However, where this information is not enough to show our compliance, or an audit is required by the ICO or another regulator, we will allow for and contribute to a proportionate audit or inspection, on at least 30 days' written notice, during business hours, subject to confidentiality, and at your cost.

4. Security and Confidentiality

We protect personal data with measures that include:

- Hosting on Google Cloud Platform in London. All customer data is stored in the UK.
- SSL/TLS encryption for every website and for access to the Cloud.
- Encrypted backups.
- Staff administrative access locked by IP firewall to approved static IP locations.
- Two-factor authentication available for your Cloud users. We recommend you switch it on.
- User permissions, so you control which of your people can see and edit each area.
- Regular software and security updates.
- Confidentiality obligations for all staff, with access to customer data only where their work needs it.
- Annual Cyber Essentials assessment.

You are responsible for the security of your own accounts. Keep passwords private, remove administrators who leave your organisation and use two-factor authentication where possible.

5. Sub-processors

You give us general authorisation to use sub-processors to deliver your services. Our current sub-processors fall into these categories:

- Cloud hosting and backup infrastructure (UK).
- Email delivery, for form notifications, newsletters and other emails sent from the Cloud.
- Payment processing, only if you take payments online. Payment providers may act as independent controllers for payment data under their own terms.
- AI content tools, only if you choose to switch them on within the Cloud.

A list of our current sub-processors by name is available on request from data@chrestos.co.uk.

We will give you at least 30 days' notice by email before adding or replacing a sub-processor. You may object on reasonable data protection grounds. We will try to resolve the objection, and if we cannot, you may end the affected service. Every sub-processor is bound by a written contract with data protection obligations equivalent to those in this DPA, and we remain responsible to you for their performance.

International transfers: your data is stored in the UK. Our email delivery provider and our optional AI tools may process data outside the UK, mainly in the United States. Where this happens we make sure the transfer is covered by appropriate safeguards under the UK GDPR, such as UK adequacy regulations (including the UK Extension to the EU-US Data Privacy Framework) or the ICO International Data Transfer Addendum. AI tools stay off unless you switch them on, and we recommend you do not enter personal data into them unless you need to.

6. Website Data Retention Schedule

As Data Controller you are responsible for approving retention periods. We are responsible for putting the agreed arrangements in place within the scope of our services. Form submissions, images and files can all be set to delete automatically after a chosen period. The periods below are our defaults and apply unless you ask us in writing for different ones.

A. Website form submissions stored in the Cloud
Retention: 30 days after submission (recommended), or the period you choose.
Responsibility: you approve the period; we set up automatic deletion.

B. Form notification emails delivered to your own inbox
Retention: in line with your own records retention policy.
Responsibility: the Customer.

C. Images, documents and other uploaded files
Retention: for as long as you need them on your website, or until an expiry date you set.
Responsibility: you review and remove content; we can set up automatic removal on request.

D. Administrator and member accounts
Retention: for as long as the account is needed.
Responsibility: you authorise and remove access; we close accounts on request and at the end of the services.

E. Shop orders, bookings and mailing lists
Retention: for as long as you need them, for example to meet accounting rules or until a subscriber unsubscribes.
Responsibility: the Customer, using the tools in the Cloud.

F. Website backups
Retention: daily database backups kept for 30 days, then one backup from each of the previous 12 months, all encrypted.
Responsibility: ThenMedia Limited.

G. Server and security logs
Retention: 90 days, for security, fault finding and preventing misuse.
Responsibility: ThenMedia Limited.

These periods are defaults only and must be reviewed and approved by you as Data Controller.

7. Data Deletion and Backups

- Automatic deletion applies to your live website database once the agreed period ends.
- Deleted database records remain in our encrypted backups until those backups expire, which can take up to 12 months. Backups are only used to recover from a fault or at your request, and if data is ever restored we will re-apply the agreed deletion.
- Uploaded files that you remove from your website are deleted from our file backups straight away. Our Backup Policy gives more detail.
- When the services end, we will delete personal data from our live systems within 30 days, unless the law requires us to keep it. Before deletion, on request, we will provide your form submissions as CSV files and copies of your uploaded files. Your website database is held in a bespoke encrypted format and cannot be transferred in full.
- On request we will confirm deletion in writing.

8. Data Breaches and Data Subject Requests

If we become aware of a personal data breach affecting your data, we will:

- Notify you without undue delay and in any event within 48 hours.
- Tell you what happened, the categories and approximate number of people and records affected, the likely consequences and the steps we have taken, adding information as it becomes available.
- Take reasonable steps to contain the breach and reduce its effects.
- Cooperate with you and, where needed, with the ICO.

You remain responsible for deciding whether a breach must be reported to the ICO (normally within 72 hours) or to the people affected.

If someone contacts us directly to exercise their rights (for example a subject access, correction or erasure request), we will pass the request to you without undue delay and will not respond ourselves except to direct them to you. We will help you find, export, correct or erase the data concerned. Many requests can be handled by you directly in the Cloud.

9. Approval and Amendments

By accepting our terms of service, you, acting as Data Controller, authorise ThenMedia Limited to process personal data in line with this DPA. You confirm that you have reviewed the Website Data Retention Schedule in Section 6 and approve the default periods, or have told us in writing which periods you want instead.

ThenMedia Limited will put the agreed retention and deletion arrangements in place within the scope of the services provided. Any change to the agreed retention arrangements must be requested or confirmed by you in writing, and we will keep a record of it.

We may update this DPA to reflect changes in the law or in our services, and will tell you about any significant change. This DPA is governed by the laws of England and Wales.

Data protection contact

Tobias Newman, Data Protection Officer
Email: data@chrestos.co.uk
Phone: 01244 478727

Authorised on behalf of ThenMedia Limited (Data Processor)

Tobias Newman, Data Protection Officer

Data Controller: the Customer, by acceptance of the terms of service
Effective date: 19 November 2026
Version: 1.0