computancy

Data Processing Agreement

How we protect personal data when we host, build, maintain or optimise your website.

October 2026 | Forms part of all Computancy service terms

IN SHORT

- You decide what personal data your website collects and why. We only handle it to provide our services, and only on your instructions.
- We keep it secure and confidential, and only people who need access have it.
- Personal data stays within the United Kingdom and the European Union.
- If a personal data breach affects your data, we will tell you within 48 hours of becoming aware of it.
- We use trusted suppliers, such as hosting and backup providers, and we tell you before we add or change them.
- When our services end, we return or delete your data, whichever you prefer.

1. About this agreement

1.1 "We", "us" and "our" mean Computancy, including anyone working on our behalf. Computancy is the trading name of Nick Warner. "You" and "your" mean the business or organisation that uses our services.

1.2 We are registered with the Information Commissioner's Office (ICO), registration number ZC279460.

1.3 This agreement applies whenever we handle personal data on your behalf while providing website hosting, development, maintenance, support, SEO or related services. It forms part of our Website Care, Hosting and Retainer Terms, our Search Engine Optimisation Terms and any other agreement for our services.

1.4 If anything in our other terms conflicts with this agreement on the subject of personal data, this agreement wins.

2. The law and our roles

2.1 We both agree to follow the data protection laws that apply, including the UK General Data Protection Regulation, the Data Protection Act 2018 and, where relevant, the EU General Data Protection Regulation.

2.2 For personal data handled through your website and systems, **you are the controller**: you decide what is collected and why. **We are the processor**: we handle it only to provide the services you have asked for.

3. What data we handle

3.1 Depending on the services you use, we may store, access, move, maintain, back up, restore, migrate, change or delete personal data held on your website or connected systems.

3.2 This can include data about your website visitors, customers, enquirers, subscribers, employees, suppliers and other people, such as names, contact details, account details, IP addresses, website activity, form submissions and order records. The Annex gives the full details.

3.3 If your website handles special category data, such as health information, please tell us. You are responsible for having a lawful basis for it, and we will agree any extra safeguards it needs.

4. Following your instructions

4.1 We only handle personal data on your documented instructions. These include your Service Order, our service terms, your support requests and your other written instructions.

4.2 Your instructions cover the routine technical work needed to provide our services, such as updates, security monitoring, backups, restores and system administration.

4.3 If the law requires us to handle personal data in any other way, we will tell you first, unless the law prevents us from doing so.

4.4 If we think an instruction would break data protection law, we will tell you straight away.

5. Confidentiality

5.1 We keep your personal data confidential. Only people who need access to deliver, secure or support our services have it, and everyone with access is bound by a duty of confidentiality.

5.2 This continues after our services end.

6. Keeping data secure

6.1 We use appropriate technical and organisational measures to protect personal data against loss, misuse, unauthorised access, change or destruction, taking into account the risks involved, as Article 32 of the GDPR requires. These include:

- professionally managed and secured hosting environments;
- access controls and strong authentication, with access limited to those who need it;
- encrypted connections, and encryption of stored data where appropriate;
- firewall protection, malware scanning and security monitoring;
- regular software updates and vulnerability management;
- regular backups, kept separately from the live website, and the ability to restore systems promptly after an incident;
- regular reviews of our security measures.

6.2 No online service can be completely free of risk. We each remain responsible for our own security obligations, including you keeping your own logins and devices secure.

7. Our suppliers (sub-processors)

7.1 We use trusted suppliers to help deliver our services, such as hosting, cloud infrastructure, backup, content delivery, email delivery, security and website management providers. You give us general permission to use suppliers like these.

7.2 We only use suppliers that give appropriate protection for personal data, and they are bound by written terms giving at least the same level of protection as this agreement. We remain responsible to you for their part in handling your data.

7.3 We keep a list of our current sub-processors and will send it to you on request.

7.4 We will tell you before we add or replace a sub-processor, with at least 30 days' notice where reasonably possible. If you have a genuine data protection concern, you may object, and we will work with you to find a solution. If we cannot, you may end the affected service.

8. Where data is stored

8.1 UK websites are hosted in the United Kingdom and EU websites in Germany. All backups are stored in the European Union.

8.2 Personal data stays within the United Kingdom and the European Union. The United Kingdom is covered by an EU adequacy decision, so no restricted transfer takes place. Our team works from within the United Kingdom and the European Economic Area.

8.3 If personal data ever needs to be transferred anywhere that data protection law restricts, we will tell you first and make sure a lawful transfer safeguard is in place. This may be an adequacy decision, the UK International Data Transfer Agreement or Addendum, or the EU Standard Contractual Clauses, together with any extra measures needed.

9. Backups and how long we keep data

9.1 Where our services include backups, we keep copies of your website files and databases so we can restore them if something goes wrong. How often backups run and how long they are kept depends on your plan.

9.2 Backups are protected by the same security measures as live data, and are only kept for as long as they are needed.

10. If something goes wrong

10.1 If we become aware of a personal data breach affecting your data, we will tell you without undue delay and in any case within 48 hours of becoming aware of it.

10.2 We will tell you what happened, what data and people are likely to be affected, the likely consequences, and what we have done or plan to do about it. If we do not have all the details straight away, we will send them as our investigation continues.

10.3 We will help you meet your own obligations to report the breach to the Information Commissioner's Office or another regulator, and to tell the people affected. As controller, you decide whether a breach needs to be reported.

11. Requests from individuals

11.1 People have rights over their personal data, such as the right to see it, correct it, delete it, restrict or object to its use, or take a copy of it. We will help you respond to these requests, as far as the nature of our services allows.

11.2 If someone contacts us directly about data you control, we will pass the request to you promptly and will not respond to it ourselves unless the law requires us to.

12. Helping you stay compliant

12.1 We will give you reasonable help with data security, breach notifications, data protection impact assessments and any consultation with a regulator, as far as the nature of our services allows.

12.2 We will give you the information you reasonably need to show that we are meeting our obligations as your processor.

12.3 We will allow and contribute to audits and inspections by you, or by an auditor you appoint. We will agree sensible arrangements so that an audit protects the security of our systems and the confidentiality of our other clients. This does not restrict any audit rights you have under the law.

13. Your responsibilities as controller

13.1 As controller, you are responsible for:

- having a lawful basis for collecting and using personal data;
- telling people how their data is used, through your privacy notice;
- getting consent where the law requires it, including for cookies;
- deciding how long data is kept, and keeping it accurate and relevant;
- managing who has access to your website and systems;
- responding to requests from individuals and regulators;
- giving us lawful instructions, and telling us about any special requirements.

13.2 Nothing in this agreement removes either party's own legal obligations.

14. When our services end

14.1 When our services end, we will return or securely delete the personal data we hold for you, whichever you choose, unless the law requires us to keep it. If you do not tell us your choice within 30 days, we will delete it.

14.2 Copies in routine backups stay protected and are deleted as the backups reach the end of their normal retention period.

14.3 Any export or transfer of your website is handled as set out in our service terms and your instructions.

15. Liability

15.1 Each of us is responsible for meeting our own obligations under data protection law.

15.2 Liability under this agreement is dealt with under the limits in our service terms, except where the law does not allow it to be limited. Nothing in this agreement restricts the rights of individuals or regulators.

16. Changes and governing law

16.1 We may update this agreement from time to time, for example when the law changes. We will tell you about any change by email in advance. No change will reduce the protection given to personal data.

16.2 This agreement is governed by the law of England and Wales, subject to any data protection law that must apply.

17. Contact

17.1 For any question about this agreement or how we handle personal data, email **help@computancy.co.uk** with "Data protection" in the subject line.

Annex: Processing details

These details apply unless your Service Order or written instructions say otherwise.

ITEM	DETAILS
Subject matter	Personal data held on or collected through websites, hosting and other systems that we build, host, maintain, support or optimise for you.
Duration	For as long as we provide our services, plus the return, deletion and backup periods set out in this agreement.
Nature of processing	Hosting, storage, transmission, access, retrieval, maintenance, changes, backup, restoration, migration, security administration and deletion.
Purpose	To provide the services you have asked for, and to keep your website and systems secure, reliable and available.
Types of personal data	Contact details, identification details, account information, IP addresses, correspondence and form submissions, order and transaction records, website activity records, and other personal data you or your website collect.
People the data is about	Website visitors, customers and prospective customers, enquirers, subscribers, members, employees, contractors, suppliers and other people whose data passes through your website or systems.
Special category data	None, unless you tell us otherwise and we agree the safeguards in writing.
Sub-processors	Hosting, cloud infrastructure, backup, content delivery, email delivery, security and website management providers. Our current list is available on request.
Locations	UK websites: hosted in the United Kingdom. EU websites: hosted in Germany. All backups: stored in the European Union.
Our registration	Registered with the Information Commissioner's Office, registration number ZC279460.

Computancy, Calfway Lane, Bisley, Stroud, Gloucestershire, GL6 7BN, United Kingdom
help@computancy.co.uk | 01453 367063 | computancy.co.uk | ICO registration ZC279460