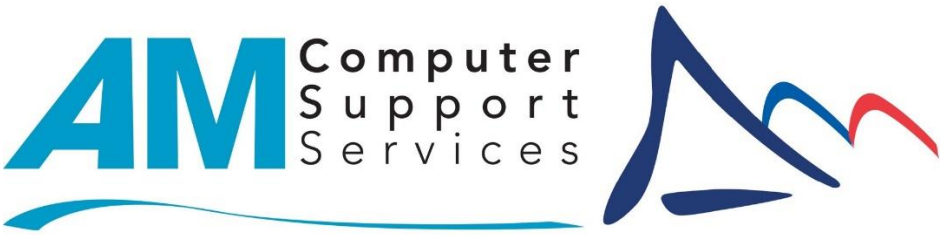

Customer Privacy Data Protection and GDPR Policy

AM CSS Ltd
Registered Office: The Mansion House, Wrest Park, Silsoe, Beds MK45 4HR
Registered in England Number 8737143

Contents

Who we are

AM CSS Ltd (“we”, “us”, “our”) is a Limited company registered in England and Wales under company number 8737143 Registered Office and trading address: The Mansion House, Wrest Park, Silsoe, Beds MK45 4HR.Our VAT number is GB 175 9482 60.

We provide IT Support and digital services such as email hosting, domain name registration, hardware and software, telecoms services and equipment, CCTV, IT consultancy and other related services.

The security of the services we provide is extremely important to us and every effort is made to protect both the information we store about customers and the data that customers store with us as part of the services we provide. Respecting privacy, responsibly managing data & personal information and transparency is part of our company’s core ethos.

.

Personal information

The information we collect is essential to the operation of our business and services that we provide to a customer, we consider this a legitimate interest. This section breaks down the information we collect, why we collect it, how it may be used and how long it is retained (where applicable). A table summary is provided at the end of this section.

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data as follows:

- **Identity Data** includes first name, last name, username or similar identifier and title.
- **Contact Data** includes billing address, delivery address, email address and telephone numbers.
- **Financial Data** includes bank account details.
- **Transaction Data** includes details about payments to and from you and other details of services you have purchased from us.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website or other systems.
- **Profile Data** includes username, purchases or instructions given, interests, preferences, feedback and survey responses.
- **Usage Data** includes information about how customers and users use our website, products and services.
- **Marketing and Communications Data** includes preferences in receiving marketing from us and our third parties and communication preferences.

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal personal identities. For example, we may aggregate Usage Data to calculate the percentage of users accessing a specific feature or service. However, if we combine or connect Aggregated Data with personal data so that it can directly or indirectly identify a person, we treat the combined data as personal data which will be used in accordance with this privacy notice.

We do not collect any **Special Categories of Personal Data** (this includes details about race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about health and genetic and biometric data). Nor do we collect any information about criminal convictions and offenses.

Contact information

When opening an account with us, we collect a customer's principal contact details; technical contact and accounts contact details (if applicable); company name (if applicable); site street addresses; postal addresses; billing address; VAT

number (if applicable). Primarily this information is used for billing purposes (e.g. invoicing) and support (ID verification, communication).

Depending on which services you have with us, some or all of this information will be shared with third-party companies as part of the performance of a customer contract – such as delivery details. The information we share is in the summary below.

As part of our General Data Protection Regulation (GDPR) compliance process, agreements are in place to ensure that privacy is maintained and that data is handled securely by all parties.

Retention

Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

However, in order to comply with corporate accounting laws, this information may be retained for a maximum of 7 years after the end of a contract. After this period, your information will be permanently removed.

Information shared with third-parties (outlined below) as part of the services we provide will retain your information as outlined by their own privacy policies. You may exercise your *right to be forgotten* by contacting our customer service.

Domain name registration, transfers & management

When managing a domain name on a customer's behalf, the customer's full name, postal address, email address, telephone number(s) is shared with our domain registration provider. Every domain name must be associated with a legal identity and as a result, your information must be provided in order to complete the registration of the domain name.

When registering a domain name on the behalf of an organisation, we may also supply the organisation's legal information (e.g. Companies House or Charity Registration number) so that the domain registry can verify the organisation's identity.

Up until the introduction of the GDPR, unless requested otherwise, contact information would have been made available in the public WHOIS database. As long as the customer address is based in the European Economic Area when registering or transferring in a domain, this information will be automatically redacted from the WHOIS database.

Should an address lie outside of the European Economic Area, it will be available on the public WHOIS database unless ID protection (domain privacy) has been chosen at the point of registration or transferral.

Please note that whilst your information may be redacted from the WHOIS, it can still be requested by law enforcement agencies or intellectual property management companies.

Without such personal information, we will be unable to register or manage the domain as this is a requirement enforced by the domain registry.

With the exception of United Kingdom (*.uk) domains, your contact information may be securely transferred outside of the Economic European Area as part of the registration process.

Digital security certificates (SSL certificates)

When you purchase a SSL/security certificate, a customer's full name, postal address, email address and telephone number may be shared with our certificate provider.

In order for a digital security certificate to perform its function, it's important that the Certificate Authority is able to verify that the certificate being issued is associated with a legal identity. In order to do this, the above information is shared with our certificate provider.

Certificates with Extended Validation (EV) may require us to supply additional information to the Certificate Authority. This will be outlined and described to a customer in detail prior to submission.

As part of this process, any information we supply as part of issuing a security certificate may be securely transferred outside of the Economic European Area.

Fraud prevention

In order to protect our network and company from fraud, your name, postal address, email address and IP address may be shared with FraudRecord and MaxMind.

Collaboration platforms

As part of our internal communication, information relating to the services we provide may be privately sent through collaborative software such as Microsoft® Office 365 systems. This information is transmitted via end-to-end encrypted channels and only accessible by members of staff or 3rd parties engaged on or contacted on a customer's behalf, such as web designers, 3rd party software support providers/licensors, hardware manufacturers/distributors, telco companies.

Ticket support

We use a self-hosted help desk solution to coordinate and track technical support requests. In order to identify a customer when requesting support, name, telephone number(s) and email address(es) are recorded in the help desk database so that we can correlate correspondence on our help desk with a customer's account.

In addition, we use a 3rd party ticket system hosted by ITarian/Comodo and such details are recorded for the same purpose. The ITarian/Comodo datacentres we use are in the EU and their privacy policy can be found here: https://www.comodo.com/repository/Comodo-Privacy-Policy-(05252018).pdf.

In addition, we employ a 3rd party answering service Telephone Answering Biz who will record similar information in order to pass on a message to us or to raise a ticket on the caller's behalf. They use a proprietary database solution hosted on their own servers and such information is not shared with other 3rd parties.

Professional services

Periodically we may need to supply access to our systems so that they can be reviewed by other professionals (e.g. accountants, solicitors, vendor or supplier support). Whilst we will not share customer information with these parties, they will have access to the information held on our systems.

In line with our company's security policy, access by third-party professionals is closely monitored and managed and only given on a case-by-case basis, ensuring access is fully revoked once the task has been completed. Where access to personal information is a requirement of the troubleshooting process, consent will be requested.

Transactional Email services

Email notifications sent from our customer portal or other control panel systems may be sent through our own in-house servers. Email delivery failures are retained for up to 30 days for troubleshooting purposes. General email is sent through the Microsoft® Office 365/Exchange system and only transaction logs are kept: the actual content of messages is not retained by the email transport system.

List of 3rd Parties/Affiliates/Partners

Microsoft®, SonicWall, HP, Lenovo, Draytek, Ubiquity, Cisco, Zyxel, Dell, Acronis, IngramMicro, Comodo, ITarian, PassPortal, ESET, BT, EE, Vodafone, IDNet, Inty, Xero, GoCardless, HSBC, FraudRecord, Ebuyer, EET, MaxMind, Telephone Answering Biz, Mayflex.

Payment information

We do not take credit or debit card payments. Customer bank account information is securely transferred to our on-line accounts system – Xero.

Direct Debit mandates are completed by customers from a link generated by our DD payment processing partner, GoCardless.

Customer user's personal information

Due to the way in which our services function, we naturally collect information about customer users as/when they access the services we provide. Customers should make their users aware that we (as the customer's service provider) collect the following information:

- IP addresses
- Browser signatures; browser name, version, operating system (user agent)
- The requested resources; Uniform Resource Identifier (URI), date/time
- Source referrer
- Contact number and email address (via the helpdesk or calls to our office)

This information is logged so that we can support you if there's a problem with your service and also to identify suspicious activity trends so that we can protect your service from malicious activity.

Data Usage Summary Table

Purpose/Activity	Type of Data	Lawful basis for processing including basis of legitimate interest
To register a new client	• Identity • Contact	Performance of a contract with a customer
To process and deliver customer's instructions including: • Processing orders to deliver the goods and services agreed. • Collect and recover money owed to us	• Identity • Contact • Financial • Transaction • Marketing and Communications	Performance of a contract with a customer Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with a customer which will include: • Notifying customers about changes to our terms or privacy policy • Asking customers to leave a review or take a survey	• Identity • Contact • Profile • Marketing and Communications	Performance of a contract with a customer Necessary to comply with a legal obligation Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)
To enable a customer to partake in a prize draw, competition or complete a survey	• Identity • Contact • Profile • Usage • Marketing and Communications	Performance of a contract with a customer Necessary for our legitimate interests (to study how clients use our products/services, to develop them and grow our business)

To administer and protect our business and communications (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	• Identity • Contact • Technical	Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) Necessary to comply with a legal obligation
To deliver relevant website content and promotions and measure or understand the effectiveness of the same	• Identity • Contact • Profile • Usage • Marketing and Communications • Technical	Necessary for our legitimate interests (to study how clients use our services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, client relationships and experiences	• Technical • Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to customers about goods or services that may be of interest	• Identity • Contact • Technical • Usage • Profile	Necessary for our legitimate interests (to develop our products/services and grow our business)

Data we process on customers' behalf

As part of providing our services, we are responsible for the physical systems and storage that contains personal information that are uploaded to the service we provide.

We fulfil the role of a *data processor* and customers are the *data controller*. As a result, we apply the same security principles and practices to the systems containing customer data as we would our own systems as a *data controller*. More information on how we protect customer data is detailed below.

Protection of data

We take security seriously and this is reflected by the policies and technologies we have in place to protect both customers' (we as a data controller) and the data customers store with us (we as a data processor).

We have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process personal data on our instructions and they are subject to a duty of confidentiality.

Technologies employed:

- stateful firewalls to strictly control traffic coming into and out of our network and equipment
- application firewalls to detect and mitigate known threats such as SQL injection and Cross-Site Scripting (XSS)
- anti-malware solutions on both Internet facing equipment (e.g. servers) and endpoint devices
- software maintenance policies to ensure all systems are up to date and quickly patched against recently discovered vulnerabilities
- enterprise grade spam & virus filtering to safeguard our company email accounts
- Data governance and retention policies to prevent accidental deletion/loss of data
- Data Loss Prevention policies on outgoing communications to prevent sharing of sensitive data
- use of strong passwords and two or multi-factor authentication on all services, equipment and devices where available
- encryption of data wherever possible, including full disk encryption on workstations, laptops & mobile devices
- ISO27001:2013 accredited data centres with 24/7 security, extensive internal & external CCTV, perimeter fencing and biometric entry systems

We use secure channels to transmit personal information and data across untrusted networks/mediums. However, customers acknowledge that the transmission of unencrypted (or inadequately encrypted) data over the internet is inherently insecure, and we cannot guarantee the security of data sent over the internet.

Customers should ensure that passwords are not susceptible to being guessed, whether by a person or a computer program. Customers are responsible for keeping their passwords used for accessing our services confidential.

Likewise, it is the customer's responsibility to ensure that you follow good security practices at all times to prevent unauthorised access to your account or service.

If/when we request access to a service (whether internal or external), you should provide it in a secure manner.

Sensitive information supplied via email should not be considered secure.

Customer rights

Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, customers and their users should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights. For the purposes of the following, the word customer also includes their users.

Principal rights under data protection law are:

A. the right to access;
B. the right to rectification;
C. the right to erasure;
D. the right to restrict processing;
E. the right to object to processing;
F. the right to data portability;
G. the right to complain to a supervisory authority; and
H. the right to withdraw consent

Customers have the right to confirmation as to whether or not we process their personal data and, where we do, request access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply a copy of such personal data. The first copy will be provided free of charge, but additional copies may be subject to a reasonable fee. Such requests should be sent to GDPR@am-css.it.

Customers have the right to have any inaccurate personal data about them rectified and, taking into account the purposes of the processing, to have any incomplete personal data about them completed.

In some circumstance's customers have the right to the erasure of personal data without undue delay. Those circumstances include: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the customer withdraws consent to consent-based processing; the customer objects to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The

general exclusions include where processing is necessary for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.

In some circumstance's customers have the right to restrict the processing of their personal data. Those circumstances are: the customer contests the accuracy of the personal data; processing is unlawful but the customer opposes erasure; we no longer need the personal data for the purposes of our processing, but the customer requires personal data for the establishment, exercise or defence of legal claims; and the customer has objected to processing, pending the verification of that objection.

Where processing has been restricted on this basis, we may continue to store the personal data. However, we will only otherwise process it: with the customer's consent; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.

Customers have the right to object to our processing of their personal data on grounds relating to their particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If a customer makes such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override the customer's interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

The customer has the right to object to our processing of their personal data for direct marketing purposes (including profiling for direct marketing purposes). If a customer makes such an objection, we will cease to process their personal data for this purpose.

The customer has the right to object to our processing of their personal data for scientific or historical research purposes or statistical purposes on grounds relating to their particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

To the extent that the legal basis for our processing of a customer's personal data is:

A. consent or;
B. that the processing is necessary for the performance of a contract to which the customer is party or in order to take steps at a customer's request prior to entering into a contract, and such processing is carried out by automated means, customers have the right to receive their personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

If the customer considers that our processing of their personal information infringes data protection laws, they have a legal right to lodge a complaint with a supervisory authority responsible for data protection. They may do so in the EU member state of their habitual residence, place of work or the place of the alleged infringement.

To the extent that the legal basis for our processing of a customer's personal information is consent, a customer has the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

A customer may exercise any of their rights in relation to their personal data by emailing GDPR@am-css.it.

Notification of a data breach

Upon discovering a breach that may have exposed a customer's personal information, we will notify the customer as soon as it's feasible using the default email address we store for the account.

Cookies

A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.

Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

Cookies do not typically contain any information that personally identifies a user, but personal information that we store may be linked to the information stored in and obtained from cookies.

We may use cookies for the following purposes:

A. authentication - we use cookies to identify a visitor to our website and as they navigate our website (cookies used for this purpose are: "WHMCSAU", "WHMCSFD", "WHMCS[string]")

B. security - we use cookies as an element of the security measures used to protect user accounts, including preventing fraudulent use of login credentials, and to protect our website and services generally (cookies used for this purpose are: "WHMCSAU", "WHMCSFD", "WHMCS[string]")

Most browsers allow users to refuse to accept cookies and to delete cookies. The methods for doing so vary from browser to browser, and from version to version. Up-to-date information about blocking and deleting cookies can be obtained via these links:

- https://support.google.com/chrome/answer/95647?hl=en (Chrome);
- https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences (Firefox);

- http://www.opera.com/help/tutorials/security/cookies/ (Opera); https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-co okies (Internet Explorer);
- https://support.apple.com/kb/PH21411 (Safari); and
- https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy (Edge)

Blocking all cookies will have a negative impact upon the usability of many websites.

Amendments

We may update this policy from time to time. We may notify customers of changes to this policy by email.