Privacy Policy

Who we are

Big Yellow Workshop t/a domainbros ("we", "us", "our") main trading address is Big Yellow Workshop, Blake House, 18 Blake Street, York, YO1 8QG .

We provide digital services such as web hosting, email hosting, domain name registration, servers, security certificates, 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 you and the data that you store with us as part of the services we provide. Respecting your privacy, responsibly managing your data & personal information and transparency is part of our company's core ethos.

You can contact us at any time on hello@domainbros.co.uk or through our customer service telephone number +44 (0)1904 378 378. You're also welcome to write to us at Big Yellow Workshop, Blake House, 18 Blake Street, York, YO1 8QG.

Key points

Our Privacy Policy breaks down the information we collect, why we collect it, how it may be used and how long it is retained. However, for your convenience, please review the below summary of our data processing practices:

- ➔ We will take appropriate technical and organisational precautions to secure your personal data and to prevent the loss, misuse or alteration of your personal data. However, you must also take precautions to protect your account & services.
- ➔ The information we collect and process is solely for the provision of services to you as a client
- ➔ All services are hosted in the UK, including backups (unless requested or stated otherwise)
- ➔ Your information will only be transferred outside of the European Economic Area if it's *strictly* required to provide a service to you & we'll ensure the information we transfer is adequately protected
- ➔ We do not sell or share your information with any third-parties unless it's a requirement of the service that we are providing (e.g. domain registration)
- ➔ We will not contact you to advertise products or services unless you have provided explicit consent, you have the right to opt-out at any time through our customer area or by contacting us using the information above.
- ➔ Alongside many other rights under the GDPR, you have the right to raise a complaint with the Information Commissioner's Office (https://ico.org.uk)

- ➔ Ensure that you regularly check our website for updates to our Privacy Policy, Terms of Service and other legal agreements for changes

Your personal information

The information we collect is essential to the operation of our business and services that we provide to you as 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).

Your IP address, requested resource & browser signature(s)

We record your Internet Protocol (IP) address, requested resource and browser signature (user agent) when accessing our website and services to help us protect your account and systems against unauthorised or malicious activity.

Retention

Your IP address(es), request(s) and browser signature(s) information will be retained for the *lifetime (definition below)* of your account. Should malicious behaviour be identified from an IP address, it will be retained indefinitely to ensure our systems are protected against further malicious activity.

Your contact information

When opening an account with us, we collect your full name, company name (if applicable), postal address, telephone number, email address and 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 contract between you and us. The exact information we share is detailed below.

As part of our General Data Protection Regulation (GDPR) compliance process, agreements are in place to ensure that your privacy is maintained and that your 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 (the "*lifetime*" of your account). 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 them directly or our customer service.

Domain name registration, transfers & management

When managing a domain name on your behalf, your 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 your 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, your contact information would have been made available in the public WHOIS database. As long as you supply an address based in the European Economic Area when registering or transferring in a domain, your information will be automatically redacted from the WHOIS database.

Should you supply an address 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.

If you do not wish to supply your 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.

Please note that many domain registries (e.g. ICANN and Nominet) are still in the process of updating their systems to be GDPR compliant. With this in mind, your information may still be temporarily public after the 25th of May deadline.

Digital security certificates (SSL certificates)

When you purchase a SSL/security certificate, your 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 you in detail prior to submission.

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

Free SSL certificates from Let's Encrypt and cPanel AutoSSL (Comodo)

Your information is not shared with SSL certificates which are supplied free of charge through Let's Encrypt or cPanel AutoSSL (Comodo).

Fraud prevention

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

Collaboration platforms

As part of our internal communication, information relating to the services we provide to you may be privately sent through collaborative software such as Slack or Google Drive. This information is transmitted via encrypted channels and only accessible by members of staff.

Ticket support

We use a hosted help desk solution (Sirportly by aTech Media Limited) to coordinate and track technical support requests. In order to identify you when requesting support, your name and email address(es) are shared with Sirportly so that we can correlate correspondence on our help desk with your account.

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 your 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, 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 a transactional email service, Amazon Simple Email Service (SES). Our Amazon SES account is configured to retain sent messages for up to 72 hours, this is to ensure messages are reliably delivered if there's a temporary problem with the email service.

Email delivery failures and successes are also retained for up to 30 days for troubleshooting purposes. Email addresses which rejected our messages are kept indefinitely to protect the reputation of the Amazon SES network and/or adhere to your email preferences.

Payment information

We do not willingly store credit, debit or bank account information on our servers. At the point of payment, your contact and card information is securely transferred to our payment providers (either Stripe or PayPal depending on your selected payment method), both PCI-DSS Level 1 compliant companies.

Your contact information is transferred to our payment provider in order to collect payment and protect against fraud.

However, for reference purposes, we store your card's last four digits and expiry date so that we can notify you if a payment has failed or your card is due to expire. This information is encrypted.

You can delete your card information on demand through our customer portal or by contacting our customer services.

Your user's personal information

Due to the way in which our services function, we naturally collect information about your users (visitors, customers etc) as/when they access the services we provide to you. You should make your users aware that we (your 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

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.

This information may also be used to generate website statistics (e.g. page views, unique visitors, most popular pages) for the benefit of the website owner and also to allow us to track service usage (e.g. bandwidth or traffic).

Data we process on your behalf

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

We fulfill the role of a *data processor* and you are the *data controller*. As a result, we apply the same security principles and practices to the systems containing your data as we would our own systems as a *data controller*. More information on how we protect your data is detailed below but as we offer a variety of services with differing service levels, please contact us if you have any specific data protection questions or concerns surrounding your services with us.

Protection of data

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

- 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
- use of strong passwords and two factor authentication on all equipment and devices
- 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, you 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.

You should ensure that your password is not susceptible to being guessed, whether by a person or a computer program. You are responsible for keeping the password you use for accessing our website and services confidential and we will not ask you for your *account* password (except when you log in to our website).

Likewise, it is your responsibility to ensure that your website and client software is actively maintained and 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), we provide a secure means of supplying sensitive information to us. This system is referred to our *credential manager*, You should use this system to exchange sensitive information at *all* times. Sensitive information supplied via via email should not be considered secure and is at your own risk.

Your rights

Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

Your 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

You have the right to confirmation as to whether or not we process your personal data and, where we do, 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 to you a copy of your personal data. You can access your personal data by visiting our customer area when logged into our website.

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

In some circumstances you have the right to the erasure of your 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; you withdraw consent to consent-based processing; you object 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 circumstances you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it: with your 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.

You have the right to object to our processing of your personal data on grounds relating to your 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 you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

You have the right to object to our processing of your personal data for direct marketing purposes (including profiling for direct marketing purposes). If you make such an objection, we will cease to process your personal data for this purpose.

You have the right to object to our processing of your personal data for scientific or historical research purposes or statistical purposes on grounds relating to your 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 your personal data is:

A. consent or;
B. that the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract, and such processing is carried out by automated means, you have the right to receive your 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 you consider that our processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. You may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement.

To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

You may exercise any of your rights in relation to your personal data by emailing us.

Notification of a data breach

Upon discovering a breach that may have exposed your personal information, we will notify you as soon as it's feasible using the default email address we store on your account. This email address can be updated through our customer area.

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 about you may be linked to the information stored in and obtained from cookies.

We use cookies for the following purposes:

A. authentication - we use cookies to identify you when you visit our website and as you 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 you to refuse to accept cookies and to delete cookies. The methods for doing so vary from browser to browser, and from version to version. You can however obtain up-to-date information about blocking and deleting cookies 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-cookies (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.

If you block cookies, you will not be able to use all the features on our website or services.

Amendments

We may update this policy from time to time by publishing a new version on our website.

You should check this page occasionally to ensure you are happy with any changes to this policy.

We may notify you of changes to this policy by email or through the private messaging system on our website.

History

As part of our transparency promise, please find the below revision history for this document.

Version: 1.0
Updated: May 2018

Revision history

- 1.0 Initial release

Questions

If you have any questions or concerns regarding our Privacy Policy, please don't hesitate to contact us and we'll be happy to address any concerns that you have regarding this policy.