



GDPR Privacy Policy

pinkdylan (partnership GF & LE Cullimore t/a), Pinkdylan Ltd and Pinkdylan Technical and Support Ltd: May 2018

Graham and Lynn Cullimore act as data controllers and processors for the above named partnership and limited companies.

HOW WE COLLECT DATA

- Website forms - enquiries and orders
- Website forms - newsletter sign-ups
- Email enquiries (and information submission)
- Telephone enquiries (and information submission)
- Telephone and Email Marketing Campaigns (TPS and GDPR respected)
- Postal enquires (and information submission)
- Face to face meetings (including exchange of business cards) (and information submission)
- Details of existing and past contracts for provision of services
- Details of quotations issued for the supply of services
- Third party referrals (with consent)
- As part of a service we supply (e.g. copywriting or photography)
- Sourcing the purchase of goods and services, and where appropriate associated maintenance and support.

WHAT DATA WE COLLECT

- Name and Position
- Company
- Nature of business
- Postal address
- Email address
- Website address
- Social media addresses
- Landline telephone number
- Mobile telephone number
- GDPR preferences (including Newsletter and Marketing sign-up requests)
- Record of email or postal communications between us
- Details of quotations we issue or receive
- Full details (including technical details) of all services we supply or receive (which may include user names and passwords, IP addresses where relevant to services we provide), may include renewal dates.
- All material supplied to us for the purposes of building and populating a website (details client dependant but may include photographs)
- Photographs taken by ourselves as a chargeable or free of charge service (which may or may not be related to the building of a website)
- All necessary accounting transaction data for purchases, sales, credits and payments.

We DO NOT collect any 'Special Information' (such as Sexuality, Religious or Political Beliefs).

WHAT WE USE DATA FOR

- Marketing to current and past clients (GDPR preferences respected)
- Marketing to prospective clients (TPS and GDPR preferences respected)
- Facilitating the provision of all pinkdylan services contracted for
- Facilitating the provision of any third party services contracted for via ourselves, such as domain name registration – in these cases provision will necessitate passing relevant personal details to the ultimate provider.

- Providing technical support (including backups) and advice to current clients in relation to services contracted for
- Providing renewal reminders for domain names and other relevant services
- Providing Newsletters to existing and past clients and anyone signing up to receive them (GDPR respected in all cases)
- Credit checks and credit control
- Maintaining financial records
- Meeting third party contractual obligations (for example, domain name registrations)
- Meeting all other legal and contractual obligations
- To help us improve the service we provide to you.

DATA THAT CLIENTS ARE RESPONSIBLE FOR

Clients are reminded that where they rent hosting facilities from us, the virtual server that we provide them with is for their own use and may well be used to store data with or without our knowledge. This will typically include:

- A record of website form replies
- Any information available on your website
- If an e-commerce platform then also records of product orders, enquiries and in contact details of the customer (or prospective customer)
- Emails

BUT could include any other data, client dependant.

Clients are responsible for controlling and processing this data in the same way as if it were on their own computers in their office.

We are able to clear down web form replies upon request, which we will do free of charge if done no more frequently than once per calendar year.

Clients are advised to delete non-active users on e-commerce sites at reasonable intervals, which is possible within their backend admin system.

We advise clients to collect Mail through POP and delete from the server at 30 days (or otherwise ensure mail is not retained on the server for extended periods).

We strongly advise clients to employ a SSL (secure certificate) which will encrypt any data sent between a users browser and the server.

Where clients set their own passwords we very strongly recommend that these are a minimum of 12 RANDOM alphanumeric characters (any new passwords we supply will equal or exceed this).

HOW WE PROTECT OUR DATA (data we hold about you, and for which we are responsible)

IN THE OFFICE (or away from office on laptop)

- All our office computers require password at boot-up, and after a (modest) period of activity
- All our office computers run full anti-virus and firewall software that is kept up to date
- All personal data saved in Excel or similar will be encrypted with password protection
- All technical data stored on our computers is encrypted and password protected
- Our accounts system requires user name and password before access can be gained

ON OUR SERVERS

- Our servers are located at a major UK data centre
- Our customer related database records are password protected and run under SS

 Web Design
  E-Commerce
  Web Hosting
  Domain Names

Tel: 01905 371041 Fax: 01905 371733 Email: hello@pinkdylan.co.uk Web: www.pinkdylan.co.uk

- Our customer related database records are only accessible from known IP addresses (i.e our IP addresses)
- Our servers are behind 2 firewalls, including brute force protection against significant attempts to log onto your server account, FTP or mail.

HOW WE **HELP** PROTECT YOUR DATA (data you are primarily responsible for, but is held on our server – including your website content, form replies, orders and email)

- Our servers are behind 2 firewalls, including brute force protection against significant attempts to log onto your server account, FTP or mail. Typically an IP address will be blocked for a period following 10 incorrect log on attempts to these services inside a 5 minute period.
- We ENCOURAGE you to use a SSL certificate, providing encryption for form replies etc. If you are not using one please contact us (there is a modest annual charge)
- We ENCOURAGE clients to collect Mail through POP and delete from the server at 30 days (or otherwise ensure mail is not retained on the server for extended periods)
- We ENCOURAGE clients not to store personal data on the server for extended periods of time, and can offer to delete web form replies on request once annually without charge. Clients must maintain customer accounts (e-commerce or product enquiry sites) as appropriate using their backend admin system
- We utilise strong passwords for all services (where we set them ourselves, where client sets them please do likewise!)
- Servers run WHM / cPanel which is regularly updated and server O/S patched as and when we are advised necessary.
- We restrict access to your website CMS / backend admin system to known IP addresses only (ours and yours), preventing the ability to update your site or view orders/customers details through guessing the password, or even if your computer is stolen with the CMS password saved it will not gain access from another location. We strongly advise you obtain a static IP address if you do not already have one.

DISCLOSURE OF YOUR PERSONAL INFORMATION

We will not disclose your personal information to any third party other than for the following reasons:

- You have requested or given us permission to do so
- We are required to do so in order for a third party to provide goods or services that you are purchasing through ourselves (such as domain names)
- It is necessary to do so in order to provide technical support in respect of services or goods we have supplied you with or are contracted to supply
- It is necessary to do so in order to receive technical support in respect of services we purchase (for example, accounts software)
- We are required to do so by law (including but not limited to VAT and tax inspections)
- To perform a credit check
- In the event we transfer all of (or a defined part of) our rights and obligations under current contracts to a third party.

ACCESSING THE PERSONAL INFORMATION WE HOLD ABOUT YOU, and DELETION REQUESTS

You have the right to request access to any personal data we may hold about you in order to ascertain the accuracy of that information. You may also be able to request deletion of such data. To apply for a 'Subject Access Request', an individual must:

- Make the request in writing (and signed) to:
Lynn or Graham Cullimore,
Pinkdylan (or Pinkdylan Ltd or Pinkdylan Technical and support Ltd)
Badgers Rest,

 Web Design
  E-Commerce
  Web Hosting
  Domain Names

Tel: 01905 371041 Fax: 01905 371733 Email: hello@pinkdylan.co.uk Web: www.pinkdylan.co.uk

Lower Farm Court,
Kinnersley,
Worcester
WR89JR

- Supply a company letterhead and we reserve the right to require further proof of identity to eliminate the risk of unauthorised disclosure
- supply appropriate information to help us locate the required information
- Where you ask us to disclose information we will retain the written request to do so even if you also request for data to be deleted. This is because we may need to prove that you requested the data disclosure.

You may challenge the data that we hold about you and, where appropriate, you may have the data corrected or request deletion. Where you are an employee of our client and wish us to remove data about you, please ask your employer for alternative contact details so we may meet our contractual obligations to our client (your employer).

We may reject subject access requests that are:

- unreasonably repetitive
- requires disproportionate technical effort (for example, developing a new system or fundamentally changing an existing practice that is not fundamentally flawed)
- risks the privacy of others
- would be extremely impractical (e.g. requests concerning information contained within backup systems, whereby deleting data may be impossible or impractical without also deleting the entire backup).

We will attempt to deliver the requested information to you within 4 weeks or receipt of request.

We may reject a request to delete data if:

- We are required to retain data by law (such as for accounting records)
- The data forms a key part of a past or current contract under which we still have a responsibility to deliver or a potential liability.

DATA RETENTION

Accounting records will be retained for a minimum period of seven years after the end of the tax year during which the final transaction for you occurs. Thereafter data may be deleted if, and only if, our accounts software facilitates deletion of old transactions without compromising the system as a whole. We will at all times retain information that we may have a legal obligation to be able to supply.

General correspondence (by email, post, and records of phone conversations) that are not relevant to any contract will usually be retained for five years.

General correspondence (by email, post, and records of phone conversations) that are relevant to any contract will usually be retained for seven years after the end of the tax year during which the contract was terminated.