Privacy Notice (General)

This privacy notice covers our main activities including our website https://www.pink-spaghetti.co.uk.

We describe here the Personal Data we collect from you when you engage with us. These are our reasons for collecting it, what we do with it and what your rights are.

Who are we?

Kelly Walsh t/a Pink Spaghetti Weybridge & Woking

You can call us on 0333 355 4926 or message us at kelly.walsh@pink-spaghetti.co.uk

We are registered as a data Controller with the Information Commissioner's Office (ICO – the UK's regulator for Data Protection), registration number ZA543240

https://ico.org.uk/ESDWebPages/Entry/ZA543240

When we talk about Data Protection Law, which laws(s) are we referring to?

- UK GDPR
- Data Protection Act 2018

  References to both laws include updates and amendments implemented by the Data (Use and Access) Act 2025

What are your rights under data protection law?

You have a number of rights relating to the processing of your Personal Data, such as asking for a copy of your Personal Data or objecting to its processing. If you would like to use them or have any questions, then please contact us.

We can't charge you for invoking your rights, however we may make a charge in the case of frequent repeat or unfounded access requests. You should expect that we will act on your request within one month of receipt, and if we anticipate that it will take longer, then we will let you know about this and explain why.

What are your specific rights?

- Awareness: You have the right to be fully informed about why and how we process your information. This privacy notice is intended to meet that requirement, but please do contact us if you have any questions. If we obtain your Personal Data from a third party (e.g. a social media platform or recruitment platform) then we will tell you where we have obtained your information from.
- Access: You have the right to a copy of the Personal Data we hold about you. It will help us to manage your request if you give us as much detail about what Personal Data you are looking for and why.
- Rectification: If you think some of the Personal Data we hold is wrong then you have the right to ask us to correct it.
- Erasure: You have the right to ask us to delete the Personal Data we hold about you. Where we are holding the Personal Data to fulfil a contract with you or your organisation then we will need to retain the Personal Data in accordance with the Personal Data retention periods shown in Schedule 2
- Restriction: You have the right to ask us to restrict the processing of Personal Data whilst we check its accuracy, if you think the processing is unlawful, if you believe we no longer need to process the Personal Data but you need us to store it due to pending legal claims, or when you object to our processing based upon our legitimate interests and we are assessing the validity of that.
- Object: Where we are processing your Personal Data based upon our legitimate interests you have the right to object to that. If your objection is valid (for instance in the case of any direct marketing activity) then we will stop processing your Personal Data for that purpose.
- Personal Data portability: You can request a copy of your Personal Data in a digital format which you can then supply to another provider when we are processing your Personal Data under the lawful basis of performing a contract with you or because we have your consent.
- Automated decisions and profiling: You have the right, in certain circumstances, not to be subject to decisions based on automated processing (including profiling) if it has a significant or legal impact on you. This doesn't apply if the processing is necessary to fulfil a contract with you, or if you have given us your consent to do so. We do not currently use any technology to make automated decisions about you.
- Complaints: You have the right to make a complaint (DPA 2018 section 164A) to us as Data controller if you consider that there is an infringement of UK GDPR in connection to Personal Data relating to you as the data subject. In order to make a formal complaint please complete this form https://forms.gle/6KenT2CmDCVNoJPS9 or request a form from our Data Protection Lead. We will acknowledge receipt of your complaint within 30 days from when the complaint is received.

The rest of this privacy notice will cover our processing activities where we act as the Data Controller and where we act as a Data Processor.

We ensure that we only process your Personal Data where it is necessary for us to do so; to deliver our services, manage our business, communicate with you or for similar reasons you would expect.
We only collect the minimum amount of Personal Data we need to properly fulfil the purpose of processing.
It is worth noting that we have a separate privacy notice specifically for employees and how we process their Personal Data.

We receive Personal Data from various different sources – the most common are from when you;

- Visit our website
- Interact with our social media channels
- Enquire about the services we offer by using our online forms, emails, social media, telephone conversations and face to face meetings
- Enquire about our employment opportunities via our website or social media channels
- Sign up to use our services by becoming a client of ours

Lawful bases for processing – General

Where we are relying on your consent you are free to change your mind and withdraw your consent at any time.
Where we are relying on our legitimate interests you are free to object to that at any time, and we'll let you know if we agree with your objection or if we don't. If we don't, we will always let you know why.
In the case of direct marketing activity, we will ensure that we cease to market our services to you should you object to our legitimate interests or withdraw your consent – for example if you unsubscribe to our newsletter.

Special category Personal Data

There are additional rules we must follow if we collect certain types of more sensitive Personal Data, known as Special Category Personal Data. These include details of

your ethnicity, beliefs, health and sexuality and in each case we must let you know why we process those Personal Data.

We do not regularly process special category or criminal behaviour Personal Data.

A full list of what we use your Personal Data for and our lawful basis for using it can be found in Schedule 1.

How long do we keep your Personal Data for?

Each purpose we identify for using your Personal Data will have its own length of time that we keep it for – we have full details of this available for you to see in our retention schedule – see Schedule 2.

Where we are relying on our legitimate interests or your consent to process your Personal Data then we will keep your Personal Data until you object to our legitimate interests (& we agree with your objection), or you withdraw your consent.

Who do we share your Personal Data with?

We will share your Personal Data if we receive a legitimate request from a law enforcement agency.
When you submit your Personal Data online your Personal Data is shared with our partners who manage our website.
If we are communicating with you via email or social media channels we will be sharing your Personal Data with those email and social media providers.
We also utilise external suppliers to provide a number of business support services. We always ensure that we have appropriate contracts in place to protect your rights when Personal Data are processed on our behalf by these third parties.
Occasionally we may share Personal Data when we are seeking external professional help from people such as our lawyers, accountants and business advisors. We will always have a legitimate reason for doing so and will maintain a record of that.
We will always ensure that appropriate protections to your rights and freedoms are in place.

For full details of which organisations we share Personal Data with and our relationship with those organisations, please see Schedule 3.

How do we keep your Personal Data secure?

- All Personal Data sent between your browser and our website are encrypted in transit.
- Where we rent or own our own servers, we ensure that they and relevant networks are encrypted. Where possible, we will encrypt Personal Data that is saved on those servers.
- Access to Personal Data is role based: only those members of staff with a legitimate need will have access.
- Systems are password protected and multi-factor authentication is enabled where available.
- We ensure that appropriate contracts are in place with our suppliers who process your Personal Data to protect your rights, to ensure that they take appropriate security measures to safeguard your Personal Data, and that any international transfers are done correctly under UK GDPR.
- Where we use different software to enable us to process your Personal Data, we ensure that where possible your Personal Data is encrypted at rest in those software.
- Our employees are all subject to an obligation of confidentiality and receive regular training on Personal Data protection matters.
- We utilise appropriate technical and organisational measures to optimise the security of your Personal Data.

For a full list of where we store your Personal Data and how it is secured, please see Schedule 3.

Cookies – for a full list of which cookies we use and how we use them please see our Cookie Notice.

Schedule 1

Purposes

Type/category of Personal Data	What Personal Data is used?	Where does this Personal Data come from?	What do you use the Personal Data for? (Purpose)	What lawful basis have we identified for using this Personal Data for this specific purpose?
Prospective Clients	Name, email address, phone number, business name, diary availability, social media profiles, enquiry notes	Website forms, email, telephone calls, Facebook, LinkedIn, networking events, referrals	Responding to enquiries, arranging discovery calls, assessing suitability for services, preparing quotations, follow up communications and CRM management	Legitimate Interests
Client	Name, business address, email address, contracts where relevant, passwords and access credentials where relevant to the services provided	Directly from the client during onboarding and ongoing service delivery	Providing contracted virtual assistant and administrative services, managing client relationships, maintaining records and service delivery	Legitimate Interests
Client Data Processed on Behalf of Clients	Names, contact details, diary information, financial information, employee information, supplier information, customer information and other Personal Data relevant to the	Client systems, databases, communications, software platforms and documents	Carrying out administrative and virtual assistant tasks on behalf of clients including inbox management, diary management, CRM updates, bookkeeping administration, spreadsheet work, research, general	None required, we act as a Data Processor on behalf of the client

	tasks instructed by the client		administration, marketing activities, LinkedIn outreach, minute taking and recruitment administration	

Schedule 2
Retention Schedule

Type of Personal Data	Purpose (What do we use the Personal Data for)?	Retention Period	Method of Destruction
Client	Managing day to day tasks	5 years post contract	Delete from software and shred any hard copy documentation
Prospect (that doesn't become a client)	Communications relating to enquiries and business development	12 months post last contact received	Delete from software and shred any hard copy documentation
Clients' Client's Personal Data	Acting on Controller's instructions	End of contract	Deleted and/or returned to the Data Controller (client)
Newsletter Subscribers	Sending marketing communications and newsletters	Until unsubscribe or consent withdrawn. Email address retained on suppression list where required to prevent future marketing communications	Delete from marketing software and shred any hard copy documentation
Financial Records	Accounting, invoicing and tax compliance	6 years in line with financial and tax record retention requirements	Delete from software and shred any hard copy documentation
Access Credentials / Passwords	Accessing client systems in order to deliver contracted services	End of contract or when access is no longer required	Delete from password management software and any related records

Schedule 3

Which organisations do we share your Personal Data with?

Name of company we share your Personal Data with	What Personal Data do we share with them?	Where are they located (Country)?	Are they a Data Processor or Data Controller?	Do they have a valid Data Processing Agreement (if a processor)? Insert link as evidence	Is the Personal Data encrypted at rest? (provide evidence – if no evidence write 'No'.
Google Workspace	Names, email addresses, calendar information, documents and communications	USA	Processor	https://workspace.google.com/terms/dpa_terms.html	Yes, https://support.google.com/googlecloud/answer/6056694
Google Meet	Names, email addresses, meeting information and communications	USA	Processor	https://workspace.google.com/terms/dpa_terms.html	Yes, https://support.google.com/googlecloud/answer/6056694
Capsule CRM	Names, email addresses, phone numbers, business information and CRM notes	UK	Processor	https://capsulecrm.com/legal/dpa/	Yes, https://capsulecrm.com/security/
Transpond	Names and email addresses used for marketing communications	UK	Processor	https://transpond.io/legal/data-processing-agreement/	Yes, https://transpond.io/security/
Mailchimp	Names and email addresses used for marketing communications	USA	Processor	https://mailchimp.com/legal/data-processing-addendum/	Yes, https://mailchimp.com/about/security/

Xero	Client names, email addresses, invoicing and financial records	New Zealand	Processor	https://www.xero.com/uk/legal/data-processing-addendum/	Yes, https://www.xero.com/uk/legal/security/
LastPass	Passwords and access credentials where relevant to service delivery	USA	Processor	https://www.lastpass.com/legal-center/data-processing-addendum	Yes, https://www.lastpass.com/security
Calendly	Names, email addresses and appointment scheduling information	USA	Processor	https://calendly.com/dpa	https://calendly.com/security
Dropbox	Names, email addresses, documents and files where used by franchisees	USA	Processor	https://www.dropbox.com/business/trust/dpa	https://help.dropbox.com/security/how-security-works