Pagefield

Ground Floor
16 Dufour's Place
London W1F 7SP

+44 (0)20 3327 4050
pagefield.co.uk

DATA PROTECTION & PRIVACY

PAGEFIELD COMMUNICATIONS LIMITED (REG NO: 07339479), 16 Dufour's Place, London, W1F 7SP

Introduction

Purpose

Pagefield is committed to being transparent about how it collects and uses third party personal data, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, how we collect and process your personal data, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of clients, suppliers, prospects, business contacts, partner agencies, marketing recipients and other personal data processed for business purposes.

This policy does not relate to employees, job applicants, contractors, volunteers, interns, apprentices or former employees. Please see the relevant People Policies

The organisation has appointed Jacqui Beaumont, Head of Finance, as its data protection officer. Their role is to inform and advise the organisation on its data protection obligations. They can be contacted at Jacqui.beaumont@pagefield.co.uk. Questions about this policy, or requests for further information, should be directed to the data protection officer.

Definitions

"Personal data" is any information that relates to an identified or identifiable natural person (ie. You as an individual). Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Contact data" means postal address, email address, telephone number

"Financial Data" means bank account details and other data necessary for invoicing or payments

How is your data collected

We collect data about you through:

- **Direct interactions**, ie filling in forms, contacting us by post, phone or email when you seek our services, make an inquiry or interact on our website
- **Third party or publicly available sources** eg information available on Google or other internet search engines and your public profile in Linkedin. Additionally we can find information from Companies House, Electoral registers and other publicly available sources.
- **Automated technology** ie as you interact with our website we may collect data about your equipment, browsing actions and patterns by our use of cookies

What data do we collect

We collect Contact Data (eg name address, phone numbers, email addresses) and Financial Data (bank account details and other data necessary for invoicing or payments). We also collect biographical data and information from Companies House, Electoral registers and other publicly available sources.

How we use your personal data

For the performance of a contract we are entering with you. This includes registering you as a client or supplier, managing payments, collecting fees, billing etc and is a legitimate interest.

Delivering relevant website content and marketing to you. All marketing materials include an option to opt-out of future marketing invites and initiatives

Making suggestions and recommendations to you about our services that may be of interest to you

Complying with a legal or regulatory obligations eg submissions to PRCA Public Affair register and the Office of the Registrar of Consultant Lobbyists

Financial record keeping for compliance with company legislation and HMRC

Cookies

You can set your browser to refuse all or some of our browser cookies. If you choose to refuse or disable cookies please note some parts of our website may not functions properly.

Sharing data

We may share data with contractors/consultants who we work with to deliver client campaigns. Any such consultants would be under a duty of confidentiality and are obliged to implement appropriate measures to ensure the security of data

We may, on occasion, share your data with our parent company PPHC who are based in the USA, to provide complimentary or similar services. We have put in place a Data Transfer Agreement with PPHC to govern any such transfers of data.

Whenever we transfer your data outside of the UK we will ensure a similar degree of protection. We do this by ensuring data is only transferred to countries that have been deemed to provide an adequate level of protection of personal data, or by using standard contractual clauses approved for use in the UK which give the transferred personal data the same protection as it has in the UK.

Data security

We have in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

Access to personal data is limited to employees who have a business need to know. Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

We have internal procedures for dealing with a suspected personal data breach and will notify you of a breach where we are legally required to do so.

Data Retention

We are required to retain data for legal, accounting and reporting requirements. The appropriate retention period is determined by the amount, nature and sensitivity of the data, and the potential risk of harm from unauthorised use or disclosure. We may store files electronically for up to ten years.

Individual rights

Individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell them:

- whether their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and
- whether the organisation carries out automated decision-making and the logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

If the individual wants additional copies, the organisation will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, the individual should send the request to Pagefield's data protection officer. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires.

The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing the organisation or causing disruption, or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override the organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to unsubscibe@pagefield.co.uk

Complaints

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

Policy Approval

This policy has been authorised by the Board of Pagefield Communications and will be reviewed every two years, but may be amended at any time should a need be identified.

Summary

Types of Personal Data	How we collect this data	Purpose	Legal Basis
Contact Details - clients	Direct Interations	Client account management	Contract
Contact Details - prospects	Direct Interations/Publicly available information	Making suggestions and recommendations to you about our services that may be of interest to you	Legitimate interest or Consent
Contact details - suppliers	Direct Interations	Conducting business with you	Contract
Contact details - other business contacts	Direct Interations/Publicly available information	Conducting business with you	Legitimate interest
Financial Data	Direct Interations	Transcating business/invoicing/payments	Contract
Biographical information	Publicly available information	Servicing client accounts	Legitimate interest
Marketing recipients	Publicly available information	Making suggestions and recommendations to you about our services / inviting you to attend events	Legitimate interest - all marketing emails have opt-out option

Last updated: October 2024