PAYNE HICKS BEACH

PRIVACY NOTICE FOR CLIENTS, INTERESTED PARTIES AND VISITORS

1. The purpose of this document

Payne Hicks Beach is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your relationship with us, in accordance with the relevant data protection rules.

It applies to clients, interested parties and visitors to our premises.

Payne Hicks Beach LLP (company number OC430964) trading as Payne Hicks Beach is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice. We are a firm of solicitors that is a licensed Alternative Business Structure, regulated by the Solicitors Regulation Authority under number. Payne Hicks Beach LLP is also used to describe Payne Hicks Beach Trustees (company number 02545358), Payne Hicks Beach Trust Corporation Limited (company number 00850087) and Payne Hicks Beach Officers Limited (company number 16104227). The registered office for these organisations is 10 New Square, Lincoln's Inn, London WC2A 3QG.

This notice applies to all clients (including prospective clients), interested parties and visitors to our premises. It does not form part of any contract to provide services. We may update this notice at any time. A copy also appears on our website (http://www.phb.co.uk) and should be drawn to the attention of any person for whom it may be relevant. Separate privacy notices have been issued for the benefit of our personnel and visitors to our website respectively, the latter being known as our website privacy policy.

It is important that you read this notice, together with any other privacy notice or privacy letter we may provide to you on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

2. Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

(a) used lawfully, fairly and in a transparent way;

(b) collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;

(c) relevant to the purposes we have told you about and limited only to those purposes;

(d) accurate and kept up to date;

(e) kept only as long as necessary for the purposes we have told you about; and

(f) kept securely.

3. **The kind of information we hold about you**

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).

There are "special categories of personal data" which require a higher level of protection.

We may collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses, date of birth, gender, marital status and dependants, family information, National Insurance number, bank account details, employment, pension and tax information, nationality and immigration status, copies of and information from identification documents such as passport and driving licence, CCTV footage and photographs. This is not an exhaustive list.

It may also be necessary for us to collect, store and use the following "special categories of personal data":

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions, trade union membership, information about your health, including any medical condition, genetic information and biometric data, and information about criminal convictions and offences.

When advising or acting for clients, we will always obtain the following information:

- Name, title, address and telephone number, information to enable us to check and verify identity (such as date of birth or passport details), electronic contact details (such as email address and mobile phone number), information relating to the matter in which our advice or representation are sought, information to enable us to undertake a credit or other financial check, financial details so far as they are relevant to the instructions (such as the source of funds and wealth if we are instructed on a purchase transaction).

The need for us to obtain additional personal data will be determined by the reason we have been instructed in relation to a particular matter.

4. **How personal information is collected**

We typically collect personal information about our clients directly from them when taking instructions. We also collect information from and about third parties in connection with those instructions. We collect personal information during the course

of acting for our clients and managing our business generally. In particular, we may collect information:

(a) from publicly accessible sources such as Companies House or HM Land Registry;

(b) directly from a third party such as:

- sanctions screening providers;
- colleagues, witnesses and family members;
- credit reference agencies; and
- client due diligence providers.

(c) from a third party such as:

- bank or building society, another financial institution or advisor;
- consultants and other professionals, including legal professionals and accountancy staff, we may engage in relation to a matter;
- employer and/or trade union, professional body or pension administrators; and
- doctors, medical and occupational health professionals;

(d) via our website (for more information, please see the cookies policy on our website);

(e) via our information technology (IT) systems such as:

- case management, document management and time recording systems;
- door entry systems, CCTV and access control systems and reception logs; and
- automated monitoring of technical systems, such as our computer networks and connections, communications systems, email and instant messaging systems.

5. How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

(a) where we need to perform the contract we have entered into with you;

(b) where we need to comply with a legal obligation; and

(c) where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

(a) where we need to protect your interests (or someone else's interests); and

(b) where it is needed in the public interest.

Situations in which we will use your personal information

Some or all of the categories of information in section 3 above are required primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

In some cases we may use your personal information to pursue legitimate interests of our own or of third parties, such as business or commercial reasons, provided your interests and fundamental rights do not override those interests. Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

We need personal information from our clients so that we may provide the legal services we have been asked to provide. If a client or potential client chooses not to provide personal data to us, we may be unable to act.

Personal data belonging to our clients and where applicable other relevant parties will also be "processed" (used) for the purposes of preventing money laundering and terrorist financing. Appropriate due diligence checks will usually include adverse media screening, which involves a review of data that is publicly available on the intranet. Checks may be conducted against prospective, previous or existing clients and other parties at our discretion.

Finally, with explicit consent, we use personal information to send marketing information we think our clients and contacts might be interested in. This may include newsletters and bulletins.

The situations in which we will anticipate we will process personal information are listed below. For general guidance, we have set out the likely situations in which personal information will be processed, the categories of data involved and the lawful bases on which processing will typically take place.

Situation	**Data category**	**Lawful processing basis**
Processing data belonging to clients for the purpose of providing legal services (including processing for internal and external auditing, investigation, regulation accreditation and taxation, quality checks, credit reference checks and business and	Basic personal contact details such as name, title, addresses, telephone numbers, and personal email addresses Date of birth Gender Family details such as marital status and details of	(i) To pursue our legitimate interest in carrying out the instructions of our clients (ii) To allow us to perform our contracts with our clients

Situation	Data category	Lawful processing basis
operational reasons such as updating and enhancing the records we hold)	dependants National Insurance number Bank account details Tax, employment and pension details and records	
	Copies of and information from identification documents such as passport and driving licence and utility bills Details from personal or professional online presence CCTV footage and photographs	
	"Special categories of personal data" such as information revealing racial or ethnic origin, religious or philosophical beliefs, health and sexual orientation, trade union membership, genetic and biometric data	(i) Explicit consent (ii) Establishing, exercising or defending legal claims (iii) Data manifestly made public by the client
	Information about criminal convictions and offences	(i) Explicit consent (ii) Establishing, exercising or defending legal claims

Situation	Data category	Lawful processing basis
Processing data belonging to interested parties for the purpose of providing legal services to clients	Basic personal contact details such as name, title, addresses, telephone numbers, and personal email addresses Date of birth Gender Family details such as marital status and details of dependants National Insurance number Bank account details Tax, employment and pension details and records	To pursue our legitimate interest in carrying out the instructions of our clients

Situation	Data category	Lawful processing basis
	Copies of identification documents such as passport and driving licence and utility bills Details from personal or professional online presence CCTV footage and photographs	
	"Special categories of personal data" such as information revealing racial or ethnic origin, religious or philosophical beliefs, health and sexual orientation, trade union membership, genetic and biometric data	(i) Explicit consent (ii) Establishing, exercising or defending legal claims (iii) Data manifestly made public by the interested party
	Information about criminal convictions and offences	(i) Explicit consent (ii) Establishing, exercising or defending legal claims

Situation	Data category	Lawful processing basis
Processing data belonging to clients and interested parties for the purpose of preventing money laundering and terrorist financing (including processing necessary to comply with professional, legal and regulatory obligations)	Basic personal contact details such as name, title, addresses, telephone numbers, and personal email addresses Date of birth Gender Family details such as marital status and details of dependants National Insurance number Bank account details Tax, employment and pension details and records Copies of and information from identification documents such as passport and driving licence and utility bills Details from personal or professional online presence CCTV footage and photographs	(i) To pursue our legitimate interest in preventing criminal activity (ii) To enable us to comply with legal obligations and exercise specific rights
	"Special categories of personal data" such as information revealing racial or ethnic origin, religious or philosophical beliefs, health and sexual orientation, trade union membership, genetic and biometric data	(i) Explicit consent (ii) Establishing, exercising or defending legal claims (iii) Data manifestly made public by the client or interested party
	Information about criminal convictions and offences	(i) Explicit consent (ii) Establishing, exercising or defending legal claims

Situation	Data category	Lawful processing basis
Processing data belonging to clients and contacts for the purpose of providing marketing information	Basic personal contact details such as name, title, addresses, telephone numbers, and personal email addresses	(i) Explicit consent (ii) To pursue our legitimate interest in assisting relevant parties and promoting our services
Processing data belonging to our suppliers for the purpose of managing our business generally	Basic personal contact details such as name, title, addresses, telephone numbers, and personal email addresses	To pursue our legitimate interest in operating effectively
Processing data belonging to visitors for the safety and security of our personnel and other visitors	Basic personal contact details such as name, title, addresses, telephone numbers, and personal email addresses CCTV footage and photographs	To pursue our legitimate interest in assisting the emergency services and protecting and assisting relevant parties
Processing data belonging to clients, interested parties and visitors for the purpose of complying with health and safety obligations	Basic personal contact details such as name, title, addresses, telephone numbers, and personal email addresses	To pursue our legitimate interest in assisting the emergency services and protecting and assisting relevant parties
	Information about health, including any medical condition	(i) Explicit consent (ii) Establishing, exercising or defending legal claims

If you do not provide personal information

If you do not provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as providing legal services), or we may be prevented from complying with our legal obligations (such as performing appropriate due diligence measures in relation to our clients).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason

is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

6. How we use special categories of personal data

"Special categories of personal data" require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal data in accordance with Articles 6 and 9 of the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) (**UK GDPR**) and the Data Protection Act 2018 in the following circumstances:

(a) in limited circumstances and not generally, with your explicit written consent; and

(b) where we need to carry out our legal obligations and in line with our data protection policy.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

When we process any special categories of personal data we shall refer you to our Appropriate Policy Document as required. Please see the Information Commission (**ICO**) website for further details. The address of the ICO website is: ico.org.uk.

Do we need your consent?

We do not need your consent if we use special categories of your personal data in accordance with our written policy to carry out our legal obligations or exercise specific legal rights. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly special categories of personal data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

7. Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so or where we have obtained your explicit consent to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions of clients and interested third parties.

We will only collect information about criminal convictions if it is appropriate given the circumstances and where we are legally able to do so. We may be notified of such information directly by you or by other people. We will use information about criminal convictions and offences in the following ways:

- to inform the way in which we act for our clients;
- to assist us in deciding whether to act or continue to act; and
- to comply with our professional or statutory obligations.

8. **Automated decision-making**

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

(a) where we have notified you of the decision and given you 21 days to request a re-consideration;

(b) where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights; and

(c) in limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any special categories of personal data, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

We do not envisage that any decisions will be taken about you using automated means. However, we will notify you in writing if this position changes. In any event, you will not be subject to decisions that have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

9. **Data sharing**

We may have to share your data with third parties, including third party service providers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK. If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We may share your personal information with third parties where required by law, where it is necessary to manage or market our business or where we have another legitimate interest in doing so.

Which third party service providers process my personal information?

Our third party service providers change from time to time and we can let you have details of parties who are processing your data at any given time upon request. We routinely share personal data with:

- professional advisers who we instruct on your behalf or refer you to (such as barristers, medical professionals, accountants, tax advisors or other experts);
- other third parties where necessary to carry out instructions (such as Companies House, mortgage providers or HM Land Registry in the case of a property transaction);
- credit reference agencies;
- our insurers and brokers, including our professional indemnity brokers, Howden;
- external auditors such as in relation to accreditation and the audit of our accounts;
- our banks;
- external service suppliers, representatives and agents that we use to make our business more efficient, (these include typing services, marketing agencies, IT support companies, document collation, analysis suppliers and software solutions used to manage data subject access requests, such as Luminance);
- adverse media, identification and verification providers that allow us to meet our legal and regulatory obligations, such as those under The Money Laundering and Terrorist Financing Regulations 2017. Providers include Creditsafe Limited and The Access Group;
- HighQ (which provides a virtual data room); and
- debt recovery organisations, such as Anthony Gold Solicitors, Legal Recoveries & Collections Limited and/or Wilkin Chapman Rollits where we deem it necessary to instruct them to obtain payment of any outstanding and overdue invoice.

Currently, the following organisations technically have access to the personal data of all clients by default:

- Mimecast (email backup);
- MJF Business Services Limited (storage of physical files and other items); and
- iManage (email and document management).

Mimecast and iManage are respected international organisations. MJF Business Services Limited store files and other items exclusively in their secure, UK facilities. We understand that these organisations provide services to many other firms of solicitors and professional advisors.

We only allow our service providers to handle your personal data if we are satisfied they take appropriate measures to protect your personal data. We also impose contractual obligations on service providers relating to ensure they can only use your personal data to provide services to us and to you.

We may disclose and exchange information with law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations.

We may also need to share some personal data with other parties, such as potential buyers of some or all of our business or during a re-structuring. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations.

How secure is my information with third party service providers?

All of our third party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business, or if it is required for legitimate business activities (or similar). The recipient of the information will be bound by confidentiality obligations. We may also need to share your personal information with a regulator or otherwise to comply with the law. Where appropriate, marketing information will be shared with specialist agencies acting on our behalf. Suppliers such as IT support companies may also have access to this information.

Transferring information outside the UK

All of our personnel are based in the United Kingdom (UK), although some may travel outside the UK from time to time. On occasion, it may be necessary to transfer the personal data that we hold about you to third parties based in countries within or outside the European Economic Area (EEA). Should it be necessary to do so, we may need to ensure that there is an adequacy regulation issued by the Secretary of State in the UK in respect of the country that we are transferring personal data to (meaning that the country is deemed to provide an adequate level of protection in accordance with the UK GDPR).

We may need to put in place appropriate measures to ensure that your personal data is treated in a way that is consistent with the UK data protection laws. Such laws are likely to include the UK GDPR and in accordance with EU laws, the EU General Data Protection Regulation (**EU GDPR**), if applicable. We may rely upon an exemption, if

it is a "one off or irregular" transfer, or put in place safeguards such as standard contractual clauses.

We have appointed IT Governance Europe Limited to act as our EU representative. If you wish to exercise your rights under the EU GDPR, or have any queries in relation to your rights or general privacy matters, please email our Representative at eurep@itgovernance.eu. Please ensure to include our firm name in any correspondence you send to our Representative.

10. Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

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

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

11. Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Our Data Retention Guidelines may be found here: http://www.phb.co.uk/compliance/data-protection.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

For the purposes of providing legal services, we will retain personal data belonging to clients in physical and electronic form for the period set out in our Data Retention Guidelines and/or correspondence. Thereafter, it will be destroyed/deleted save for

some basic information, which will usually include our client's name and address and a brief description of the matter we were contacted about. We will in any event retain information for regulatory and professional reasons, including the need for us to be able to:

- respond to any questions, complaints or claims;
- check for any conflict of interest or confidentiality issues which might arise;
- demonstrate that we treated people fairly; and
- keep records required by the law or our regulators.

For the purposes of preventing money laundering and terrorist financing, we will keep clients' identification and proof of address documents and relevant due diligence material for the same period as any files relating to matters on which we have been instructed. We usually keep original documents or certified copies.

If you would like us to send you marketing information, we will keep your contact details on our marketing list until you tell us that you no longer wish to receive this.

Please refer to our Data Retention Guidelines for information about how long we keep different kinds of data.

Upon the expiry of any retention period, data will be deleted or destroyed without further notice. We will not, of course, destroy any items which belong to a client and which we have been asked to return or deposit in safe custody.

12. **Rights of access, correction, erasure, and restriction**

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it;
- request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- request the erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to stop processing personal information where we are relying on a legitimate interest and there is something about your particular situation which makes you want to object to processing on this ground;

- request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it; and
- request the transfer of your personal information to another party.

This is not a comprehensive list of your rights and further information is available from the ICO, whose contact details are set out below. You are also entitled to discuss your rights with an independent solicitor.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our Data Protection Officer (**DPO**) (whose details are provided below) in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

13. **Right to withdraw consent**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. If you are a client, this may mean that we are no longer able to act for you.

You also have the right to withdraw or amend your direct marketing preferences or to update your contact details for marketing purposes at any time.

To withdraw your consent, please contact our DPO (whose details are provided below) or any partner at the firm or e-mail us at marketing@phb.co.uk or write to us at Marketing, Payne Hicks Beach LLP, 10 New Square, Lincoln's Inn, London WC2A 3QG.

Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law or/and are required to process such data for our regulatory or compliance purposes.

Upon withdrawal of your consent to receive direct marketing information, we will further remove all of your personal data from our marketing lists. We will also

endeavour to remove your personal data from any other party with whom we may have shared it.

14. Data protection officer

We have appointed a DPO to oversee compliance with this privacy notice. Our DPO is Jonathan Sewell (telephone 020 7465 4388 or email client.services@phb.co.uk). If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the ICO, the UK authority for data protection issues.

You can obtain further information about your rights from a solicitor or from the ICO. You have the right to complain to the ICO (telephone 0303 123 1113 or email casework@ico.org.uk) about the way in which your personal data is processed.

You also have the right to seek a judicial remedy.

15. Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

10 New Square, Lincoln's Inn, London WC2A 3QG
DX Box 40 London, Chancery Lane
Tel: 020 7465 4300 Fax: 020 7465 4400 www.phb.co.uk
VAT registration number: GB 232 667364
The Firm is a licensed Alternative Business Structure, regulated by the Solicitors Regulation Authority
SRA number: 807106
© Payne Hicks Beach LLP: 23 November 2026