PRIESTLEYS PRIVACY NOTICE

This is the Privacy Notice for Priestleys Limited (trading as Priestleys, Attorneys at Law). It sets out the basis on which any personal information we collect from you, or that you provide to us, will be processed by us. It is important that you read this Privacy Notice in full to understand what information we hold about you, how we may use it and what rights you have in relation to your data.

By giving us your personal information, directly or through third parties, and by using the services that we provide, you are accepting and consenting to our processing of your personal information in accordance with the practices described in this Privacy Notice.

The Data Protection Act 2017 came into force in the Cayman Islands on 30 September 2019. We may need to update this policy to reflect any further changes in the law, as well as any changes to our business from time to time. Please check this policy regularly to ensure you are familiar with its terms. This policy was last updated on 13 July 2022.

WHO WE ARE

We are Priestleys Limited (trading as Priestleys Attorneys-at-Law), a resident Cayman Islands company incorporated and registered under the laws of the Cayman Islands. Our registered address is Second Floor, Building C, Caribbean Plaza, 878 West Bay Road, P.O. Box 30310, George Town, Grand Cayman, KY1-1202, Cayman Islands.

In this Privacy Notice we refer to ourselves as "**we**", "**us**", "**our**" and "**Priestleys**".

Priestleys is a "data controller". This means that we are responsible for deciding how we hold and use personal information we have collected from you, including:

- how to use, store, and process your personal data;
- with whom to share your personal data;
- when to modify or erase your personal data;
- when to engage one or more third parties to process your personal data; and
- which such third parties to engage.

We have appointed a data protection officer ("**DPO**") who is responsible for overseeing questions in relation to this Privacy Notice. If you have any questions about this Privacy Notice, including any requests to exercise your legal rights, please contact our DPO using the details set out below:

By post: The Data Protection Officer, Priestleys, P.O. Box 30310, Grand Cayman KY1-1202, Cayman Islands

By email: data.protection@priestleys.ky

IMPORTANT DEFINITIONS

Personal data, or **personal information**, means any information about an individual from which that person can be identified. This includes name, contact details (both personal and business), identification number, location data, an online identifier (such as a social media username), biographical or physical information.

Sensitive personal data means information about racial or ethnic origin; health; sexual orientation or sex life; political, philosophical or religious beliefs; genetic or biometric data; and criminal convictions.

What personal data do we collect and process?

We may obtain and process different kinds of personal data about you in the course of providing legal and other services to you, which we have grouped together follows:

- **Identity Data** includes first name, last name, nationality, marital status, title, date of birth, tax identifier and tax residence.

- **Contact Data** includes home and/or business addresses, email addresses and telephone numbers.
- **Transaction Data** includes information obtained by providing legal and other services to you, details about services provided by us to you, details of payments to and from you, and other details of our interactions including correspondence and conversations.
- **Employment Data** includes details about who you work for and your role in any such organisation, your employment history and your credentials.
- **Financial Data** includes bank account and payment card details.
- **Social Data** includes information about your family, lifestyle and social circumstances.
- **Public Data** includes publicly available information such as details on Government registries or otherwise publicly available on the Internet.

In addition to the categories of personal information listed above, we may collect sensitive personal information (also known as special categories of data) about your racial or ethnic origin; your political affiliations; your physical or mental health, such as information that may be revealed in a medical exam required for immigration purposes; or information relating to criminal offences or convictions.

We use this data to ensure that our products and services are delivered appropriately. For example, we may need medical and criminal data about you as part of the process of applying for a work permit on your behalf.

We will only obtain and use sensitive personal data where we need to and where data protection law allows us to do so. We will ask for your specific informed consent at the time of collecting sensitive data. Where you provide consent for us to process sensitive personal information, you have the right to withdraw this consent at any time. We will apply additional security and confidentiality measures when processing your sensitive personal information.

How is your personal data obtained?

We use different methods to collect data from and about you including through:

Direct interactions. You may give us your personal data (including sensitive personal data) through any number of direct interactions. This includes personal data you provide when you:

- make an enquiry about our services;
- instruct us to provide legal or other services and during the provision of legal or other services;
- correspond with us by post, phone, email, social media or otherwise;
- When you fill in our forms and any associated documentation that you complete when enquiring about, or to engage us in providing, our services;
- When you talk to us on the phone or face to face when you visit our offices to enquire about or to engage us in providing our services;
- provide feedback or respond to surveys; and
- register for, attend, or participate in events or seminars hosted or provided by us.

Third parties or publicly available sources. We may receive or obtain personal data about you from various third parties and publicly available sources such as:

- fraud prevention and detection agencies;
- Government and public bodies, including tax authorities, governmental agencies and departments and law enforcement;
- organisations or businesses that refer you to us, such as other law firms, other clients, accountants, or financial institutions; and
- other professional advisors, financial institutions, expert witnesses, courts and tribunals, mediators, and others with whom we interact in connection with the services that we provide to you.

Failure to provide information

Where we need to collect personal data by law (for example in order to carry out identity verification and anti-money laundering checks), or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have entered into with you or we may be unable to comply with our own legal obligations.

In some cases, a failure to provide information when requested may delay our provision of legal or other services to you and in other cases, we may be unable to act for you or may have to withdraw from acting.

How will we use your information?

The main reason why we process your personal data is to be able to provide you with legal or other services as instructed by you.

Personal data will be processed by us where you consent to the processing or where that processing is necessary for (1) the performance of a contract with you; or (2) compliance with a legal obligation to which we are subject; or (3) the purposes of our legitimate interests (or those of a third party).

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal basis we rely on to do so. We have also identified what our legitimate interests are, where appropriate. A legitimate interest is when we have a business or commercial reason to use your information. However, our use of your personal data must not have a negative or unfair impact on you.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.

Purpose	Legal Basis	Legitimate Interest (where relevant)
To provide you with legal services To provide you with other services such as company secretarial or the provision of a registered office address for your company	Performance of a contract Legitimate interests	To pursue commercial objectives, including running our business profitably and efficiently To exercise our rights under a contract with you To keep our client and other records up to date
To manage our relationship with you, including: • fulfilling our contractual obligations; • managing payments, fees and charges; • collecting and recovering money owed to us; • dealing with client complaints; and • notifying you of any changes to our terms of business or privacy notices.	Performance of a contract Legitimate interests	To exercise our rights under a contract with you To manage credit control and debt recovery To manage complaints or potential claims To fulfil our responsibilities to our clients
To carry out identity verification and fraud prevention checks,	Legal obligation	To prevent fraud or money laundering

background checks and anti-money laundering procedures	Legitimate interests	To protect our business and reputation
To improve and develop our services	Legitimate interests	To improve our services and our efficiency
To manage our business, including: • financial management and administration; • business planning; • corporate governance; • audits	Legal obligation Legitimate interests	To improve our services and our efficiency To operate an efficient and profitable commercial business
To comply with relevant legal obligations To comply with reporting obligations to regulatory bodies	Legal obligation	
Capture CCTV footage for security, quality and training purposes	Legitimate interests	Our legitimate interests around health and safety and crime prevention and detection
To protect the rights, property, or safety of our staff, our clients, or others	Legal obligation Legitimate interests	To manage the safety of our staff, clients and others
To establish, exercise or defend our legal rights	Legitimate interests	To enforce our legal rights

With whom do we share your personal data?

There may be circumstances in which we need to share your personal data with third parties. The third parties to which we may transfer your personal data include:

- other third parties to any transaction, dispute, legal proceeding or other legal matter on which we are advising you (including other professional advisers, external counsel, expert witnesses, courts and tribunals, surveyors etc.);
- our service providers who provide IT and system administration services (including client management systems, data rooms and other software services);
- our agents and service providers who we engage in the provision of our services, including professional advisers, bankers, surveyors, external counsel, insurers, auditors, and others;
- fraud prevention agencies;
- any relevant regulatory authority;
- the police and any other law enforcement agencies;
- public registers and public information resources, such as the Cayman Islands Land Registry or the Cayman Islands Register of Companies; and
- third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets.

Any sharing of your personal data will only take place either where we are legally obliged to do so, where it is necessary for the performance of a contract with you or where it is in our legitimate interests to do so, including as follows:

- to maintain network and information security;
- to undertake reference checks, credit checks and risk assessments;
- to protect and defend our legal rights;

- if the structure of Priestleys changes in the future. We may choose to sell, transfer, or merge parts of our company, or our assets; or we may seek to acquire other companies or merge with them. During any such restructuring of our business, we may share your information with other parties. We will only do this if those parties agree to keep your data safe and private; and
- to pursue our commercial objectives where this does not override your rights and freedoms as a data subject.

International transfers

We process all personal data relating to clients within the Cayman Islands.

We will only send your personal data outside of the Cayman Islands:

- where you instruct us to do so, including where we are required to do so as part of the legal services that you have instructed us to provide (for example when we deal with professional advisors outside of the Cayman Islands on your behalf or when we deal with counterparties to a transaction or other legal matter outside of the Cayman Islands on your behalf);
- where we are instructed on your behalf by someone outside of the Cayman Islands (for example your professional advisors outside of the Cayman Islands);
- where we need to do so in order to comply with our or your legal obligations;
- where the transfer is necessary for reasons of public interest; or
- where the transfer is necessary for the establishment, exercise or defence of legal rights.

Whenever we transfer your personal data outside of the Cayman Islands, we will seek to ensure that it is protected to a similar degree as within the Cayman Islands by using appropriate safeguards, which may include the following:

- we will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission;
- where the recipient organisation is not located in a country with an adequacy decision by the European Commission, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe; and
- where the recipient organisation is based in the USA, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the European Union and the USA.

The safeguards used will depend on the circumstances of the transfer and the location of the recipient.

Automated-decision making or profiling

We do not use automated decision-making (including profiling) to make any decisions which would produce a legal or similarly significant effect on you.

How long do we retain your personal data?

We will retain your personal data for as long as necessary to fulfil the purposes for which the personal data was obtained and to comply with any legal, accounting or reporting requirements.

Generally speaking, we will keep your client files (and any personal data contained therein) for a minimum period of 10 years following completion of the matter, so that we are able to respond to a question, complaint or claim. We will keep the information used to verify your identity, and other related client due diligence information, for five years after you cease to be our client. We may keep your data for longer than 10 years if we cannot delete it for legal, regulatory or technical reasons. If we do, we will make sure that your privacy is protected and only used for those purposes.

Retention periods for records are determined based on the type of record, the nature of the service or advice that we have provided, and any applicable legal or regulatory requirements. The rules that apply to determine how long it is appropriate to hold client files can be complex and varied. If you require further information about our retention periods, please contact our DPO using the contact details above.

For example, the rules concerning prevention of money-laundering mean that if any of your personal information forms part of "know your client" records, we will have to retain it for as long as we continue to have a client-advisor relationship with you (if you are a private client) or the relevant corporate client (if you are a business owner), and then for several years following the end of that client-advisor relationship.

MARKETING

We may use your personal information to tell you about our services. This is what we mean when we talk about 'marketing'.

The personal information we have for you is made up of what you tell us and data we collect from third parties we work with. We use this to identify and inform us of what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you.

We can only use your personal information to send you marketing messages if we have either your consent or a 'legitimate interest'. That is when we have a business or commercial reason to use your information. It must not unfairly go against what is right and best for you.

You can ask us to stop sending you marketing materials by contacting our DPO any time using the contact details above.

Before sending electronic marketing communications, we will follow the law and guidance which requires us to seek your consent. You can withdraw your consent at any time.

We may ask you to confirm or update your choices from time to time and if there are changes in the law, regulation, or the structure of our business.

Priestleys will never sell your personal data to third party organizations for marketing purposes.

ACCURACY OF YOUR DATA

It is important that the personal data we hold about you is accurate and up to date. Please keep us informed if your personal data changes during your relationship with us.

DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those agents, contractors and other third parties who have a business need to know.

They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and the Cayman Islands Ombudsman of a breach where we are legally required to do so.

Y**OUR RIGHTS**

Priestleys is committed to upholding your data privacy rights.

The right to be informed

We will be open and transparent about how and why we use your personal information. This will be set out in our privacy notices.

The right of access

You have the right to ask us what personal information we hold about you and to request a copy of your personal information. This is known as a 'subject access request' ("**SAR"**).

SARs need to be made in writing and accompanied by proof of your address and identify. If someone is requesting information on your behalf, they will need to provide us with your written consent for us to release your information and proof of ID (both yours and theirs).

If you are seeking to obtain specific information (e.g. about a matter or that relates to a specific time period), please clarify the details of what you would like to receive in your written request.

We will provide a copy of your information free of charge. However, we can charge a 'reasonable fee' if your request is manifestly unfounded or excessive, particularly if it is repetitive. Our fee will be based on administrative costs incurred by us in providing your information.

Where your request is manifestly unfounded or excessive, we can refuse to respond. If we refuse to respond to your request, we will let you know why.

We have 30 days to provide you with the information you have requested (although we will try to provide this to you as promptly as possible). We may extend this period if your request is complex or we have received several requests from you. If this is the case, we will inform you within one month of the receipt of your written request, explaining why an extension is necessary.

The right to rectification

You can ask us to rectify your personal data if it is inaccurate or incomplete by contacting us using the contact details above. If you do, we will take reasonable steps to check its accuracy and correct it.

Where we have shared your personal data in question with others, we will contact each recipient and inform them of the rectification of your personal data, unless this proves impossible or involves disproportionate effort.

Please help us to keep our records accurate by keeping us informed of any changes in your personal information.

The right to stop or restrict processing

You have the right to require that our processing of your personal data stops, or does not begin, or ceases for a specified purpose or in a specified way. This is not an absolute right, and we will need to consider the circumstances of any such request and balance this against our need to continue processing the data, for example, to comply with a legal obligation. If we are processing your data on the grounds of legitimate interests (as detailed earlier), we will consider whether our legitimate grounds override those of yours.

Your request needs to be made in writing. We have 21 days to comply with your request (although we will try to do this as promptly as possible). We may write to the Ombudsman requesting permission not to comply with this request if we believe we need to continue processing your data, for example, to comply with a legal obligation.

Where we have shared the personal data in question with others, we will contact each recipient and inform them of the cessation or restriction of the personal data, unless this proves impossible or involves disproportionate effort.

The right to stop direct marketing

You have an absolute right to ask us to stop processing your personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing. You must notify us in writing.

This is an absolute right and there are no exemptions or grounds for us to refuse. If we receive an objection from you to us processing your personal information for direct marketing purposes, we will stop processing your data for that purpose. If we are only holding your personal information for marketing purposes, we will erase that information.

If you feel we have not complied with your request, you have the right to complain to the Ombudsman (whose contact details are below).

Rights in relation to automated decision making and profiling

You can ask us to review any decisions that are determined by automated means (making a decision about you solely by automated means without any human involvement). You can also object to our use of your personal data for profiling (automated processing of personal data to evaluate certain things about you). Please contact us on the contact details above.

The right to complain/seek compensation

You have the right to complain to the Ombudsman if you believe we have breached or are in violation of the Data Protection Act. You can complain on your own or someone else's behalf. If you are complaining on behalf of another, you must provide us with written authorization from that person.

If you suffer damage as a result of us violating the Data Protection Law, you may seek compensation in the courts.

If you wish to exercise any of these rights, please contact our DPO using the details above.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

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

COMPLAINTS

You have the right to complain to the Cayman Islands Ombudsman, which regulates the processing of personal data, about how we are processing your personal data.

If you are unhappy with why or how we have used your personal information, please contact our DPO using the contact details above.

Alternatively, if you want to raise a complaint about our processing of your data or would like to seek an independent view, you can contact the Cayman Islands Ombudsman using the following contact details:

Information Commissioner,
Ombudsman Cayman Islands
info@ombudsman.ky
Website: www.ombudsman.ky

PRIESTLEYS
Attorneys at Law

Subject Access Request Form

Application for access to your personal data held by Priestleys Attorneys at Law ("Priestleys")

Your Subject Access Rights
Subject to certain exceptions, you have a right to have access to and/or correct any personal information that Priestleys holds about you (your "**personal data**"). If you wish to make a Subject Access Request, please complete this form carefully and follow the instructions regarding the provision of proof of identity and details of how to return the form to Priestleys. The purpose of this form is to ensure that all necessary information to complete your Subject Access Request is provided to Priestleys. You are not obliged to use this form, but if you do not, please ensure that all necessary information on this form is provided. You will not usually need to pay a fee to access your personal data. However, if your request is unfounded or excessive, we may charge a reasonable fee for complying with your request, or we may refuse to comply.

The term "**data subject**" refers to the person about whom the information is being requested

Section 1 – Details of the data subject

Title (please tick one)	☐Mr ☐Mrs ☐Miss ☐ Ms Other ☐ (please state)……
First Name	
Family Name	
Date of Birth (dd/mm/yyyy)	
Gender	☐Male ☐Female

Current Address	
Telephone number	
Email address	

Section 2 - Are you the data subject?

☐Yes If you are the data subject, please go to Section 4	☐No If you are acting on behalf of the data subject, please go to Section 3

Section 3a - Details of the person requesting the information (if different to Section 1)

Title (please tick one)	☐Mr ☐Mrs ☐Miss ☐ Ms Other ☐ (please state)……
First Name	
Family Name	
Company (if applicable)	
Address	
Telephone number	
Email address	

Section 3b – Relationship with data subject.

Please describe your relationship with the data subject that leads you to make this request on their behalf:

Section 3c – Authority to release information

A representative must obtain authority from the data subject before personal data can be released. The representative should obtain the data subject's signature below or provide a separate note of authority. This must be an original signature, not a copy (tip: using blue ink often helps verification). If the data subject lacks capacity to give authority in this way, the representative should provide evidence of the authority that it has, such as proof of legal guardianship for children under 12 or a power of attorney. I hereby give my authority for the representative named in Section 3 of this form to make a Subject Access Request on my behalf under the General Data Protection Regulation (Regulation (EU) 2016/679)	
Signature of Data Subject: ……..	Date: ……..

Section 4 – Proof of Identity.

In order to prove the data subject's identity, we need to see copies of two pieces of identification, one from list A and one from list B below. Please indicate which ones you are supplying. Please do not send originals. In addition, if you are acting on the data subject's behalf, we also need to see evidence of your identity. Please send us two pieces of identification, one from list A and one from list B below.	
List A (one from below) Passport/Travel Document Photo driving licence National Identity Card	**List B (plus one from below)** A letter sent to you by Priestleys Utility bill showing current home address Bank statement

Section 5 – Details of the data required

Please provide as much detail as you can about the personal data you are requesting to help us locate it quickly (continuing on a separate sheet if necessary):
Are there any specific dates you require this information to relate to? Please state: …… …… …… ……

Section 6 – Declaration

The information which I have supplied in this application is correct, and I am the person to whom it relates or a representative acting on his/her behalf. I understand that Priestleys may need to obtain further information from me/my representative in order to comply with this request.

Signature of Data Subject/Representative:……..Date:……

Please return the completed form
by post to:
The Data Protection Officer
Priestleys Attorneys-at-Law
P.O. Box 30310
Grand Cayman, KY1-1202
Or by email to: data.protection@priestleys.ky

Voluntary Information

It would be helpful for us to know the reasons for your request, as this information will help us to improve our service (this is voluntary so you don't have to provide any reason and it will have no bearing on the processing of your subject access request): …….. …….. …….. …….. …….. …….. …….. ……..