

GLOBAL PRIVACY NOTICE

We need to tell you about the types of data we process about you, what we do with your data, and why we do it. The purpose of this Notice is to provide you with helpful information in this regard.

If you have any questions, or if you want any further information, you can contact us using the details provided at the end of this Notice.

WHO ARE WE?

Addleshaw Goddard is a global business and is committed to complying with applicable data protection laws wherever we operate. We want this Notice to be as clear and concise for you as possible, wherever in the world you happen to be. As such, we have tried to use general terminology rather than refer to technical language that may vary from country to country.

The **AG Group** consists of Addleshaw Goddard LLP and any entities owned or controlled by Addleshaw Goddard LLP or any of its partners, or owned or controlled by any other AG entity or any of such AG entity's partners, including Addleshaw Goddard (GCC) LLP, Addleshaw Goddard (Germany) LLP, Addleshaw Goddard (Europe) LLP, Addleshaw Goddard (Ireland) LLP, Addleshaw Goddard (Luxembourg) LLP, Addleshaw Goddard (Middle East) LLP, Addleshaw Goddard LLC and Nasser Al Habsi & Saif Mamari Law Firm.

WHAT TYPES OF DATA DO WE PROCESS?

We process personal data about lots of different categories of people, including our clients and prospective clients, people who have a connection with the matters we act on for our clients, people we or our staff have relationships with, people who work for our suppliers, people who may want to work with us, people who visit our offices and other people not directly connected to the AG Group who interact with us (either directly or through our website).

Because of the nature of the services we provide, the types of data we process can be quite varied, but will usually include your name and contact details. Depending on the nature of our relationship with you, we may also process information about your connection with our clients and other organisations; identification (including copies of your passport or driving licence); financial affairs; family, lifestyle and social circumstances; education and employment background; the services we provide to you or your business; your preferences (including when visiting our offices); your relationship with our staff; the goods or services you or your company provide to us; and your use of our website (including login information to online systems we use).

In some circumstances we may process "special category" or "sensitive" personal data about you, in which case we take particular care to only process such data in accordance with the strict legal parameters. This type of data can include information about your health; racial, ethnic and communal origin; religious, philosophical or political beliefs; trade union membership; sex life or sexual orientation; or genetic or biometric data. We may also process personal data relating to criminal convictions and offences.

HOW DO WE COLLECT OR OBTAIN YOUR DATA?

We may obtain personal data from you directly, from our clients, from people and organisations involved in matters we act on for our clients, from public sources and from others, such as recruitment agencies, regulators, suppliers and professional bodies.

Where you are our client:

- it will sometimes be necessary for you to provide us with information directly, and in those cases it is your responsibility to ensure that all such information is materially complete and not misleading. The accuracy and appropriateness of our advice may be affected as a consequence of your failure to do so;

- you may also provide us with personal data about other people. Please ensure you provide them with a copy of this Notice, where appropriate to do so;
- if any information changes, please let us know so that we can keep it updated on our systems;
- please see the specific section below relating to the client due diligence information we collect.

WHAT DO WE DO WITH YOUR DATA?

We process personal data for the purpose of providing legal services to our clients, managing our relationships with clients and potential clients and also for our own general business purposes, which may include:

- fraud prevention, anti-money laundering, anti-bribery and the prevention or detection of crime;
- ensuring the safety and security of our people, systems and premises (where we also use CCTV);
- disclosures to our auditors, our own legal and other professional advisors, our banks, insurers, and insurance brokers;
- administering our clients' accounts with us, including providing e-billing services and tracing and collecting any debts;
- managing our business performance, assessing client satisfaction (such as by asking client representatives to participate in surveys), enhancing the client experience, conducting specific tests on or developments to our existing or new systems, networks, applications and software, and general improvement of our services;
- advertising, marketing and public relations, including sending you direct marketing communications (insofar as we are permitted by law) and facilitating events – see further details below.

WHAT BASIS DO WE HAVE FOR PROCESSING YOUR DATA?

We will only process your personal data where we have a lawful basis for doing so. The "lawful bases" for processing are set out in applicable data protection law and, depending on the relevant circumstances and jurisdiction, our processing will be on the basis of one or more of the following:

- the performance of a contract to which you are a party or in order to take steps at your request prior to entering a contract;
- compliance with our legal obligations;
- for our legitimate interests (this includes carrying out the business of providing legal services and pursuing our general business interests);
- the establishment, exercise or defence of legal claims;
- to carry out tasks in the public interest/reasons of substantial public interest;
- to comply with laws relating to anti-money laundering or counter-terrorist financing obligations or the prevention, detection or prosecution of any crime.

In addition, in some circumstances we may process personal data on the basis that you have provided your consent, for example, through instructing us on a matter (including, in some instances, in respect of "special category" or "sensitive" personal data about you). Please note that you have the right to withdraw any such consent, which you can do by getting in touch with us using the contact details below.

WHO DO WE SHARE YOUR DATA WITH?

In providing services to our clients, operating our business and in complying with our legal obligations, we may share the personal data that we obtain about you, insofar as we are permitted by law, with the following:

- members of the AG Group;
- others involved in any matter, including courts, tribunals, counterparties, experts, private investigators, and other third parties involved in a matter;
- suppliers and service providers used by us in providing services, details of which can be made available on request, including postal services, document storage facilities, front of house teams and IT service providers such as cloud providers of software as a service, data room providers and providers of our IT servers;
- financial organisations, and debt collection, credit reference and tracing agencies;
- our auditors, our own legal and other professional advisors, our banks, insurers and insurance brokers;

- government and law enforcement agencies (including tax authorities), regulators (for example the UK Information Commissioner); and
- our and your trade associations, professional bodies and business associates.

HOW LONG DO WE KEEP YOUR DATA?

We keep personal data in accordance with our internal retention procedures, which are determined in accordance with our regulatory obligations and good practice. These retention periods depend on the nature of the information (for example, we apply different retention periods to our staff information as opposed to information on our client files), and are subject to change.

If you have any questions in this regard, or any concerns about how long we keep your information for, please contact us using the details below.

CLIENT & THIRD PARTY DUE DILIGENCE

As a law firm subject to certain requirements under anti-money laundering/counter-terrorist financing regulations, we are required to obtain client due diligence information and documentation (**CDD**) in order to comply with our regulatory requirements. For the purposes of this notice, CDD also includes any information and/or documentation we are required to obtain about third parties connected with our client matters from whom we receive funds or to whom we send funds (which we may do in very limited circumstances).

The CDD, which may include personal data about you, may be obtained from you directly or from publicly available sources or third party information providers (such as company and risk intelligence databases).

In some cases, we will use a third party system called Amicus ID to collect CDD. Amicus ID enables you to upload the necessary CDD via an online portal. Please note the following:

- **Facial Similarity Check:** You may be asked to complete a facial similarity check on Amicus ID. This involves you uploading a photo of your ID documentation and a video of yourself. A digital comparison will be made to verify your identity. You will be asked to provide your consent to the processing of this data before accessing Amicus ID. For more information about how your data is processed on the Amicus ID system, please see their privacy policy: <https://amicus.co/policies/privacy>.
- **Credit Reference Agency Check:** We may also confirm your identity using a credit reference agency, which may leave a "soft foot print" on your record, showing that someone in the legal sector has searched your record.

We process CDD for the purpose of complying with our regulatory obligations, including for the prevention of money laundering and terrorist financing.

Our lawful basis for this processing will generally be that such processing is necessary for the performance of a task carried out in the public interest, that the processing is necessary for compliance with a legal obligation to which we are subject, and/or that the processing is necessary for reasons of substantial public interest (or as otherwise stated in this Notice). Where a facial similarity check is conducted via Amicus ID, you will be asked to provide your consent to the processing of this data.

Please note that we require CDD in order to determine whether we can accept you as a client, proceed with a particular instruction from you (including assessing any third parties associated with the instruction), and/or receive funds from, or send funds to, a third party connected with a client matter. Therefore, if you do not provide the CDD we have requested, we may be unable to provide services to you (or receive funds from you/send funds to you, as the case may be).

YOUR USE OF OUR WEBSITE: COOKIES

Cookies are small text files that can be placed on your computer by websites to make your experience more efficient and also to provide useful insights to the website owner.

Rather than repeat the details in this Notice, we would invite you to review the [Cookie Policy on our website](#) for details about the Cookies we use, what personal data we may process as a result, and your choices in this regard.

DIRECT MARKETING

We may use your contact details to send you marketing materials, provided we are permitted to do so by law. You always have the right to unsubscribe from any marketing. You can do so by clicking on the relevant link in the next email we send you, or by contacting us directly using the details below.

Our marketing emails may contain cookies or similar technology to enable us to understand how you have interacted with our content including whether and when you opened our email and whether you have visited our website as a result. We may use this information as part of limited profiling in relation to your engagement with our events and content. Please see our [Cookie Policy](#) for more details. If you are unhappy with this, please ensure you unsubscribe from our marketing.

ATTENDANCE AT EVENTS

When you attend events or meetings arranged by us, you may choose to provide us with details of your dietary requirements. That information could reveal other information concerning, for example, your religious beliefs or health. Please note that we may pass this information on to our catering teams where necessary, some of whom will be third parties contracted by the Firm. You have the right to withdraw your consent to our processing of this information at any time by contacting us using the details below.

At some events there may be a photographer and/or film-maker present and the images they provide may be used for publicity and marketing purposes. This might include use in printed and online marketing, social media and press releases. If you would prefer us not to use your image, please contact the event organiser or speak to one of our staff on site at the event.

When we hold an event in conjunction with a third party or where, for example, we have a guest speaker, we may share details as to who is attending or has been invited to the event with those parties.

VIRTUAL EVENTS AND MEETINGS

We regularly host events, webinars and meetings using online platforms such as Microsoft Teams, Kaltura, and Go To Webinar.

When you register for one of these events or attend a meeting, the system we use will sometimes record details, including the time that you joined and left a call and how you interacted with the session. We may use this data to better understand the popularity of, and engagement with, our events and content.

In some instances, an event or meeting will be recorded in which case you will see or hear an automated notification. Generally, our purpose for recording a webinar or training session will be to enable us to share a session with further participants or provide a copy to attendees. We will only do this where appropriate, taking into account our data protection and client confidentiality obligations.

Where we record a meeting, this may be for the purposes of subsequently typing up a record of the discussion, particularly where this is necessary for our own records or in the fulfilment of services to our client. We will usually delete the recording once we have created and saved a transcription. However, in some instances we may retain a copy for longer insofar as is necessary.

DATA ROOMS & ONLINE PLATFORMS

As part of our work (including knowhow sharing) for our clients, you may be invited to access an online platform (for example, HighQ) to review or access documents and information or to upload information yourself. To the extent we have access to any personal data about you in connection with this, we will treat that personal data in accordance with this Notice.

Please ensure you review any other privacy information provided to you in connection with these services or platforms, including information provided by the third parties who provide the platforms. You must also ensure you read and comply with the relevant terms of use.

E-SIGNATURES

In order to make signing contracts easier, we may use e-signature software. This involves inputting your contact details into third party e-signature software (**DocuSign**) and uploading the relevant contract for signature, which may contain personal data about you. In general, the data will be stored on servers within the European Economic Area (see Storage and Transfers of Data below) and will be deleted following a short retention period.

WHAT ARE YOUR RIGHTS?

You have rights under data protection laws to request from us access to, rectification of, or erasure of your personal data. You also have the right to request the restriction of any processing or to object to our processing of your personal data. Finally, you have the right to data portability. Please use the contact details in the "How can you contact us?" section below to exercise your rights.

If you have a complaint about our processing of your personal data, please follow the [Complaints Procedure](#) on our website (a hard copy is available on request).

You may also have the right to lodge a complaint with the regulator in the jurisdiction where the relevant AG Group member operates. You can find more information about lodging a complaint, and about your rights more generally, at the following websites:

- for the United Kingdom, please see the Information Commissioner's website: www.ico.org.uk
- for Hamburg, please see the Hamburg Commissioner for Data Protection and Freedom of Information: www.datenschutz-hamburg.de
- for Ireland, please see the Irish Data Protection Commissioner's Office: www.dataprotection.ie
- for Luxembourg, please see the National Commission for Data Protection: <https://cnpd.public.lu/>
- for Paris, please see the National Commission for Data Protection and Freedom: www.cnil.fr
- for the Dubai International Financial Centre, please see the Commissioner of Data Protection's website: www.difc.ae
- for the Qatar Financial Centre, please see the Data Protection Office website: www.qfc.qa/en/operating-with-qfc/data-protection
- for Singapore, please see the Personal Data Protection Commissioner's website: www.pdpc.gov.sg

STORAGE AND TRANSFERS OF DATA

We are committed to complying with our obligations under data protection law in relation to the security of your personal data, including by having appropriate technical and organisational measures in place to help protect personal data against unauthorised processing and accidental loss, destruction or damage.

In general, we will process your personal data:

- in the country within which the relevant AG Group member operates; and
- within the United Kingdom.

In some instances, we may also use third party software that stores data in another jurisdiction. Usually, this will be within the European Economic Area, and, in any case, this will always be carried out in accordance with applicable data protection laws. Where required, we ensure that appropriate safeguards are in place in respect of any transfer of personal data outside of a particular jurisdiction, which may include the agreement of "standard contractual clauses" with the relevant data importer.

Some of our third party software suppliers provide support services from various international locations and, in some rare instances, it may be necessary for individuals providing that support to have sight of, or access to, stored personal data. As above, this will always be conducted strictly in accordance with applicable data protection laws such that appropriate safeguards are implemented.

The AG Group operates worldwide and as a result your personal data may be processed by any members of the AG Group. Where data is transferred between members of the AG Group, this is conducted strictly in accordance with applicable data protection law. Where required, we have agreed "standard contractual clauses" between members of the AG Group to provide appropriate safeguards for such transfer. A copy of these can be made available to view on request.

HOW CAN YOU CONTACT US?

You can get in touch with us in respect of any of the members of the AG Group, and in relation to any data protection queries, by contacting our Office of the GC (which has general oversight of our compliance with data protection laws). You can:

- email us at DataProtection@addleshawgoddard.com or DataProtection@aglaw.com.
- write to us at the Office of the GC, Addleshaw Goddard LLP, Milton Gate, 60 Chiswell St, London EC1Y 4AG, United Kingdom
- submit a query via our website using the General Enquiries Form on the Contact Us page: <https://www.addleshawgoddard.com/en/contact-us/>

For jurisdictions where we have a Data Protection Officer, your correspondence will be passed on to them for a response, as appropriate.

This notice was last updated 12 March 2024.

MORE IMAGINATION MORE IMPACT

addleshawgoddard.com