

Data Protection Privacy Note:

1. The business of **MANUEL JESUS DOÑA MARTIN**, of 41 Whitehall, London SW1A 2BY trading as **MANUEL MARTIN & ASSOCIATES** (“**Business**”, “**we**”, “**us**”, “**our**”). The Business is registered with the Information Commissioner’s Office (“**ICO**”) under number Z7569080.
2. If you have any questions about this privacy notice (“**Notice**”), please contact us by [email](#).
3. The Business will process your and third parties’ personal data, as further explained below, in the course of providing you with notarial, legal and associated services, including access to our website and online features (“**Services**”).
4. We will let you know by posting on our website or otherwise, if we make any changes to this Notice from time to time. Your continued use of the Services after notifying such changes will amount to your acknowledgement of the amended Notice.
5. **PLEASE NOTE:** You shall and you hereby agree to indemnify the Business and its affiliates and their officers, employees, agents and subcontractors (each an “**Indemnified Party**”) from and against any claims, losses, demands, actions, liabilities, fines, penalties, reasonable expenses, damages and settlement amounts (including reasonable legal fees and costs) incurred by any Indemnified Party arising out of or in connection with any breach by you of the warranties included in paragraph 8.

What is Personal Data?

6. “**Personal data**” means any information relating to an identified or identifiable natural person, known as ‘**data subject**’, who can be identified directly or indirectly; it may include name, address, email address, phone number, IP address, location data, cookies and similar information. It may also include “**special categories of personal data**” such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a data subject, data concerning health or data concerning a natural person's sex life or sexual orientation.
7. The Business may process personal data and special categories of personal data which you provide in connection with the Services about yourself and other data subjects, e.g. individuals whose details are included in any materials provided by you to the Business. The Business may obtain information about you and other data subjects from third party service providers, such as due diligence platforms. If you use our online Services, the Business may collect information about your devices including clickstream data.
8. The provision of certain personal data is mandatory in order for the Business to comply with mandatory client due diligence requirements and consequently to provide the Services. You warrant on a continuous basis that such personal data is accurate, complete and up to date. Failure to comply may result in documents being rejected by the relevant certification authorities, held invalid in the destination country or other difficulty to successfully completing the Services.
9. In relation to personal data of data subjects you warrant to the Business on a continuous basis that:
 - (a) where applicable, you are authorised to share such personal data with the Business in connection with the Services and that wherever another data subject is referred to, you have obtained the explicit and demonstrable consent from all relevant data subjects to the inclusion and use of any personal data concerning them;
 - (b) to the extent this is required in connection with the Services, such personal data is accurate, complete and up to date; and
 - (c) either you provide your explicit consent and warrant that each data subject has provided explicit consent for the transfer of personal data to foreign organisations in connection with the Services, or that an alternative legal gateway for such transfer (such as transfer necessary for the conclusion or performance of a contract concluded in the interest of the data subject) has been satisfied.

How do we use your personal data?

10. The Business will only process personal data, in accordance with applicable law, for the following purposes:
 - (a) **responding to your queries, requests and other communications;**
 - (b) **providing the Services**, including, where applicable, procuring acts from foreign organisations;
 - (c) **enabling suppliers and service providers to carry out certain functions on behalf of the Business in order to provide the Services**, including webhosting, data storage, identity verification, technical, logistical, courier or other functions, as applicable;
 - (d) **allowing you to use features on our website**, when you choose to do so;
 - (e) **sending you personalised marketing communications** requested by you, as well as **servicing personalised advertising to your devices**, based on your interests in accordance with our Cookie Statement below. You have the right to disable cookies as set out above or to unsubscribe by emailing us;
 - (f) **ensuring the security of the Business and preventing or detecting fraud;**
 - (g) **administering our Business**, including complaints resolution, troubleshooting of our website, data analysis, testing of new features, research, statistical and survey purposes;
 - (h) **developing and improving our Services;**
 - (i) **issuing invoices, manage accounts and records, and collection of payments and debts;**
 - (j) **complying with applicable law**, including Notary and/or Solicitors Practice Rules, guidelines and regulations or in response to a lawful request from a court or regulatory body.

For example, where a Solicitor knows or suspects that a transaction on behalf of a client involves money laundering or terrorist financing, the Solicitor is under a legal duty to disclose information to the National Crime

Agency. If, while we are acting for you, it becomes necessary to make a money laundering disclosure, we won't be able to inform you that a disclosure has been made, the reasons for it or that this is the reason for any delay in your case. If we do we ourselves commit a Criminal Offence!

The legal basis for our processing of personal data for the purposes described above will typically include:

- processing necessary to fulfil a **contract** that we have in place with you or other data subjects, such as processing for the purposes set out in paragraphs (a), (b), (b) and (d);
- your **consent**, such as processing for the purposes set out in paragraph (e);
- processing necessary for our or a third party's **legitimate interests**, such as processing for the purposes set out in paragraphs (a), (b), (b), (f), (g) and (h), which is carried out on the basis of the legitimate interests of the Business to ensure that Services are properly provided, the security of the Business and its clients and the proper administration of the Business; and
- processing necessary for compliance with a **legal obligation** to which we are subject, such as processing for the purposes set out in paragraph (j).and
- any other applicable legal grounds for processing from time to time.

What exactly are cookies?

11. In order to collect the information including personal data as described in this Notice, we may use cookies and similar technology on our website. A cookie is a small piece of information which is sent to your browser and stored on your computer's hard drive, mobile phone or other device. You can set your browser to notify you when you receive a cookie. This enables you to decide if you want to accept it or not. However, some of the Services offered through our website may not function properly if your cookies are disabled.

12. Cookies can be first party or third party cookies.

- First party cookies – cookies that the website you are visiting places on your device.
- Third party cookies – cookies placed on your device through the website but by third parties, such as, Google.

The cookies on our website

13. We may use the following cookies on our website:

- Strictly necessary cookies. These cookies are essential in order to enable you to move around our website and use its features. Without these cookies, Services you have asked for cannot be provided. They are deleted when you close the browser. These are first party cookies.
- Performance cookies. These cookies collect information in an anonymous form about how visitors use our website. They allow us to recognise and count the number of visitors and to see how visitors move around the website when they are using it and the approximate regions that they are visiting from. These are first party cookies.
- Functionality cookies. These cookies allow our website to remember choices you make (such as your user name, language or the region you are in, if applicable) and provide enhanced, more personal features. These cookies can also be used to remember changes you have made to text size, fonts and other parts of web pages that you can customise. The information these cookies collect may be anonymised and they cannot track your browsing activity on other websites. These are first party cookies.
- Targeting or advertising cookies. These cookies allow us and our advertisers to deliver information more relevant to you and your interests. They are also used to limit the number of times you see an advertisement as well as to help measure the effectiveness of advertising campaigns. They remember that you have visited our website and may help us in compiling your profile. These are persistent cookies which will be kept on your device until their expiration or earlier manual deletion.
- Social Media cookies. These cookies allow you to connect with social media networks such as LinkedIn and twitter. These are persistent cookies which will be kept on your device until their expiration or earlier manual deletion.

14. We may combine information from these types of cookies and technologies with information about you from other sources.

Cookie consent and opting out

15. We assume that you are happy for us to place cookies on your device. Most Internet browsers automatically accept cookies. However, if you, or another user of your device, wish to withdraw your consent at any time, you have the ability to accept or decline cookies by modifying your browser setting. If you choose to decline cookies, you may not be able to fully experience the interactive features of our website, our platforms and Services.

16. When you arrive on our website a pop-up message will appear asking for your consent to place advertising cookies on your device. In order to provide your consent, please click '*I understand*'. Once your consent has been provided, this message will not appear again when you revisit. If you, or another user of your device, wish to withdraw your consent at any time, you can do so by altering your browser settings otherwise we will assume that you are happy to receive cookies from our website. For more information please visit www.allaboutcookies.org and <http://www.youronlinechoices.com/uk/>.

Disclosure of personal data

17. There are circumstances where the Business may wish to disclose or is compelled to disclose your personal data to third parties. These scenarios include disclosure to:

- our **subsidiaries** or **associated offices**;
- our **suppliers** and **service providers** to facilitate the provision of the Services, including couriers, translators, IT consultants and legalisation and other handling agents, webhosting providers, identity verification partners (in

order to verify your identity against public databases), consultants, for example, in order to protect the security or integrity of our business, including our databases and systems and for business continuity reasons;

- **public authorities** to carry out acts which are necessary in connection with the Services, such as the Foreign Office;
- **foreign organisations** to carry out acts which are necessary in connection with the Services, such as Embassies, Consulates and High Commissions;
- **professional organisations** exercising certain public functions in relation to the notaries profession, such as Chambers of Commerce;
- subject to your consent, our **advertising and marketing partners** who enable us, for example, to deliver personalised ads to your devices or who may contact you by post, email, telephone, SMS or by other means;
- **successor or partner legal entities**, on a temporary or permanent basis, for the purposes of a joint venture, collaboration, financing, sale, merger, reorganisation, change of legal form, dissolution or similar event relating to a Business. In the case of a merger or sale, your personal data will be permanently transferred to a successor company;
- **public authorities** where we are required by law to do so; and
- **any other third party** where you have provided your consent.

International transfer of your personal data

18. We may transfer your personal data to a third party in countries outside the country in which it was originally collected for further processing in accordance with the purposes set out above. In particular, your personal data may be transferred to foreign organisations such as foreign Embassies located in the UK or abroad. Such organisations will process personal data in accordance with the laws to which they are subject and international treaties over which the Business has no control.
19. If the Business transfers personal data to private organisations abroad, such as subcontractors, it will, as required by applicable law, ensure that your privacy rights are adequately protected by appropriate technical, organisation, contractual or other lawful means. You may contact us for a copy of such safeguards in these circumstances.

Retention of personal data

20. Your personal data will be retained for as long as is reasonably necessary for the purposes listed above or as required by the law. For example, the Notaries Practice Rules require that that notarial acts in the public form shall be preserved permanently. Records of acts not in public form shall be preserved for a minimum period of 12 years. Please contact us for further details of applicable retention periods. Personal data may for reasons of security and convenience be stored on remote data facilities but in an encrypted form.
21. We may keep an anonymized form of your personal data, which will no longer refer to you, for statistical purposes without time limits, to the extent that we have a legitimate and lawful interest in doing so.

Security of personal data

22. The Business will implement technical and organisational security measures in order to prevent unauthorised access to your personal data.
23. However, please be aware that the transmission of information via the internet is never completely secure. Whilst we can do our best to keep our own systems secure, we do not have full control over all processes involved in, for example, your use of our website or sending confidential materials to us via email, and we cannot therefore guarantee the security of your information transmitted to us on the web.

Data subject rights

24. Data subjects have numerous rights in relation to their personal data. For further information about your data protection rights please visit the ICO [website](https://ico.org.uk). (<https://ico.org.uk>)
 - **Right to make a subject access request (SAR).** Data subjects may request in writing copies of their personal data. However, compliance with such requests is subject to certain limitations and exemptions and the rights of other data subjects. Each request should make clear that a SAR is being made. You may also be required to submit a proof of your identity and payment, where applicable.
 - **Right to rectification.** Data subjects may request that we rectify any inaccurate or incomplete personal data.
 - **Right to withdraw consent.** Data subjects may at any time withdraw their consent to the processing of their personal data carried out by the Business on the basis of previous consent. Such withdrawal will not affect the lawfulness of processing based on previous consent.
 - **Right to object to processing, including automated processing and profiling.** The Business does not make automated decisions. Profiling may be carried out for Business administration purposes, such as monitoring trends in user visits of our website, and in order to deliver targeted ads. The Business may use third party due diligence platforms which provide recommendations about data subjects by automated means. We will comply with any data subject's objection to processing unless we have a compelling overriding legitimate ground for the processing, the processing is for the establishment, exercise or defence of legal claims or we have another lawful reason to refuse such request. We will comply with each valid opt-out request in relation to marketing communications.
 - **Right to erasure.** Data subjects may request that we erase their personal data. We will comply, unless there is a lawful reason for not doing so. For example, there may be an overriding legitimate ground for keeping the personal data, such as, our archiving obligations that we have to comply with.

- **Restriction.** Data subjects may request that we restrict our processing of their personal data in various circumstances. We will comply, unless there is a lawful reason for not doing so, such as, a legal obligation to continue processing your personal data in a certain way.
- **Right to data portability.** In certain circumstances, data subjects may request the controller to provide a copy of their personal data in a structured, commonly used and machine readable format and have it transferred to another provider of the same or similar services. To the extent such right applies to the Services, we will comply with such transfer request. Please note that a transfer to another provider does not imply erasure of the data subject's personal data which may still be required for legitimate and lawful purposes.
- **Right to lodge a complaint with the supervisory authority.** We suggest that data subjects contact us about any questions or complaints in relation to how we process personal data. However, each data subject has the right to contact the relevant supervisory authority directly.

If you provide services to our Notary Business you agree to comply with the data processing terms ("**Terms**") set out below. Your attention is particularly drawn to clause 8 of the Terms. To the extent of any conflict, the Terms shall prevail over any services agreement or other agreement between you and our Manuel Martin & Associates (our Business) in relation to the services.

DATA PROCESSING TERMS

In order that you as a service provider and data processor (referred to as "**Processor**" or "**you**" or "**your**") may provide or continue to provide certain services (the "**Services**") to us, Manuel Martin & Associates and data controller (referred to as "**Business**" or "**we**", "**us**" or "**our**"), you have agreed that these data processing terms ("**Terms**") shall apply (notwithstanding any other terms and conditions applicable to the delivery of the Services to the contrary) in order to address the compliance obligations imposed upon us and our Clients pursuant to the Data Protection Law. These Terms shall constitute a separate agreement or they may be incorporated by reference in the relevant Services agreement, as the case may be.

BY ACCEPTING ANY MATERIALS FROM THE NOTARY BUSINESS OR OTHERWISE COMMENCING THE SERVICES ("EFFECTIVE DATE"), YOU AGREE THAT THE PROCESSOR WILL PROCESS NOTARY BUSINESS PERSONAL DATA IN ACCORDANCE WITH THESE TERMS, WHICH YOU HEREBY ACCEPT FOR AND ON BEHALF OF THE PROCESSOR.

NOW IT IS HEREBY AGREED as follows:

1. definitions

In this Agreement, capitalised words shall have the meaning as set out below or, as the case may be, elsewhere in this Agreement:

"Affiliate" - means any entity that directly or indirectly controls, is controlled by, or is under common control with, a party from time to time during the Term;

"Data Protection Law" - means the data privacy laws applicable to the processing in connection with the Services, including, where applicable, the Directive 95/46/EC, as amended or replaced by any subsequent Regulation, Directive or other legal instrument of the European Union including by the General Data Protection Regulation or similar law, or the applicable data privacy laws of any other relevant jurisdiction;

"Client" - means any client of Manuel Martin & Associates;

"Contractual Clauses" - means the standard contractual clauses of the European Commission for the transfer of personal data across borders, as amended or replaced from time to time, or any equivalent set of contractual clauses approved for use under Data Protection Law; and

"Manuel Martin & Associates' Personal Data" - means the personal data processed by Processor in connection with the Services on behalf of Manuel Martin & Associates during the Term. The processing may include activities auxiliary to our notarial or legal services, such as postal, courier, legalisation, translation, hosting, administrative and other services. This will include names and other information about data subjects included in Client materials; and

The words "**data subject**", "**personal data**", "**processing**" and variations, "**controller**" and "**processor**" shall have the meaning attributed to them in Data Protection Law.

2. APPOINTMENT

Our Business is designated by its Clients, Client Affiliates and our Business Affiliates (collectively "**Instructing Parties**") to provide and manage various services, including the Services on their behalf. Accordingly, our Business Personal Data may contain personal data in relation to which Instructing Parties are controllers. Our Business confirms that it is authorised to communicate to Processor any instructions or other requirements on behalf of Instructing Parties in respect of processing of our Business Personal Data by Processor in connection with the Services.

Processor is appointed by our Business to process our Business Personal Data on behalf of our Business and/or the Instructing Parties, as the case may be, as is necessary to provide the Services or as otherwise agreed by the parties in writing.

3. DURATION

The Terms shall commence on the Effective Date and shall continue in full force and effect until such time as all Services have ceased and all our Business Personal Data in the Processor's possession or within its reasonable control (including those held by a Subprocessor) has been returned or destroyed (the "Term").

4. Data Protection COMPLIANCE

In relation to its processing of our Business Personal Data, save as otherwise required by law, you agree to: process our Business Personal Data only as required in connection with the Services and in accordance with our documented lawful instructions from time to time; inform us if, in your opinion, an instruction infringes Data Protection Law; ensure that all personnel authorised by you to process our Business Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; implement appropriate technical and organisational measures to appropriately safeguard our Business Personal Data having regard to the nature of the personal data which is to be protected and the risk of harm which might result from any Security Breach (as defined below), at a minimum the measures set out in the Schedule; promptly inform us of any data subject requests under Data Protection Law or regulatory or law enforcement requests relating to our Business Personal Data. You shall not acknowledge or otherwise respond to the subject access request except with our prior written approval, which shall not be unreasonably withheld; provide such assistance as our Business may reasonably require in order to ensure our or the Instructing Parties' compliance with Data Protection Law in relation to data security, data breach notifications, data protection impact assessments and prior consultations with the Information Commissioner's Office or other competent authority; at our choice, without delay delete or return all our Business Personal Data to us, and delete existing copies of all our Business Personal Data in the Processor's possession or within its reasonable control (including those held by a Subprocessor); and make available to our Business information reasonably necessary to demonstrate your compliance with these Terms and allow for, and contribute to, audits and inspections carried out by our Business.

5. SUBPROCESSORS

Processor will sub-contract, outsource, assign, novate or otherwise transfer obligations under these Terms or engage any subcontractors involved in the processing of our Business Personal Data (each a "Subprocessor") only with our Business's prior written consent and subject to clause 2.

When engaging a Subprocessor, Processor will:

carry out reasonable due diligence; enter into a contract on terms, as far as practicable, same as those in these Terms, and which may include Contractual Clauses to provide adequate safeguards with respect to the processing of our Business Personal Data; and inform us of any intended changes concerning the addition or replacement of a Subprocessor from time to time. If we object to any such change on reasonable grounds, then acting in good faith the parties will work together to resolve such objection.

6. SECURITY INCIDENTS

"Security Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, our Business Personal Data transmitted, stored or otherwise processed.

Processor will notify our Business without undue delay if Processor aware of any Security Breach.

Processor will investigate the Security Breach and take reasonable action to identify, prevent and mitigate the effects of the Security Breach. Processor will take such further action as we may reasonably request in order to comply with Data Protection Law.

Processor may not release or publish any filing, communication, notice, press release, or report concerning any Security Breach ("Notices") without our prior written approval; such approval shall not be unreasonably withheld.

7. INTERNATIONAL DATA TRANSFERS

Processor will ensure that none of our Business Personal Data are transferred out of either:

the European Economic Area; or

any other territory in which restrictions are imposed on the transfer of our Business Personal Data across borders under Data Protection Laws,

without the prior written consent of our Business and subject to clause 7.2.

Our Business will ensure that Contractual Clauses or other applicable transfer mechanism, such as EU-US Privacy Shield Framework in relation to EU-US transfers, is in place to ensure adequate level of data protection.

8. INDEMNITY

Notwithstanding any provisions of the relevant Services agreement to the contrary, Processor shall and hereby agrees to indemnify Notary Business and Instructing Parties and their officers, employees, agents and subcontractors (each an "Indemnified Party") from and against any claims, losses, demands, actions, liabilities, fines, penalties, reasonable expenses, damages and settlement amounts (including reasonable legal fees and costs) incurred by any Indemnified Party as a result of any gross negligence or wilful breach by Processor of these Terms.

9. MISCELLANEOUS

Clause and other headings in these Terms are for convenience only and shall not affect the meaning or interpretation of these Terms.

To the extent of any conflict, these Terms shall prevail over any Services agreement or other agreement.

Nothing in these Terms will exclude or limit the liability of either party which cannot be limited or excluded by applicable law. Subject to the foregoing sentence, (i) these Terms, including any appendices, constitutes the entire agreement between the parties pertaining to the subject matter hereof and supersedes all prior agreements, understandings, negotiations and discussions of the parties relating to its subject matter; and (ii) in relation to the subject matter of these Terms neither party has relied on, and neither party will have any right or remedy based on, any statement, representation or warranty, whether made negligently or innocently, except those expressly set out in these Terms.

Processor shall agree any amendment to these Terms that may be required from time to time for us and Instructing Parties to comply with any amended Data Protection Laws.

All notices of termination or breach must be in English, in writing and addressed to the other party's primary contact person or legal department. Notice will be treated as given on receipt, as verified by a valid receipt or electronic log. Postal notices will be deemed received 48 hours from the date of posting by recorded delivery of registered post.

The provisions of these Terms are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of these Terms shall remain in full force and effect.

These Terms are governed by English law and the parties submit to the exclusive jurisdiction of the English courts in relation to any dispute (contractual or non-contractual) concerning these Terms save that either party may apply to any court for an injunction or other relief to protect its property or confidential information.

SCHEDULE: Security measures

Processor shall put in place the following measures, as applicable.

Minimum technical measures

Firewalls which are properly configured and using the latest software;
user access control management;
unique passwords of sufficient complexity and regular expiry on all devices;
secure configuration on all devices;
regular software updates, if appropriate, by using patch management software;
timely decommissioning and secure wiping (that renders data unrecoverable) of old software and hardware;
real-time protection anti-virus, anti-malware and anti-spyware software;

- https;
- encryption of all portable devices ensuring appropriate protection of the key;
- encryption of personal data in transit by using suitable encryption solutions;
- multi-factor authentication for remote access;
- WPA-TKIP secured WiFi access;
- delinquent web filtering and other appropriate internet access restrictions;
- intrusion detection and prevention systems;
- appropriate and proportionate monitoring of personnel; and
- data backup and disaster recovery measures and procedures.

Minimal organisational measures

- Vet all personnel including staff, contractors, vendors and suppliers (including Subprocessors) on continuous basis;
- non-disclosure agreements used with all personnel;
- regular training of all personnel on confidentiality, data processing obligations, identification of Security Breaches and risks;
- apply principle of least authority, including a restricted or strictly controlled transit of data and material outside of office;
- physical security on premises including reception or front desk, security passes, clean desk policy, storage of documents in secure cabinets, secure disposal of materials, CCTV, etc.;
- apply appropriate policies including Information Security Policy, Data Protection Policy, BYOD, Acceptable Use Policy;

limited and monitored personal use of work resources, as appropriate.