

## DATA PROTECTION POLICY

### INTRODUCTION

This Policy ("**Policy**") sets out the 9 Data Protection Principles which **G S Notary Public Limited** (company registration number 09608778) ("**Business**") commits to comply with when processing personal data in the course of its business of providing notarial services.

The Business has notified its data processing activities to the Information Commissioner's Office under registration number: ZA351211.

The Appendix contains a Glossary of the defined terms in this Policy.

### COMPLIANCE WITH THIS POLICY

The Business will ensure the protection of personal data in accordance with this Policy by the Notary, all Personnel and Suppliers.

A breach of data protection laws by the Notary, any Personnel or Supplier could result not only in monetary penalties awarded against the Business but also negative publicity which could affect the Business as well as the entire notaries' profession.

### THE DATA PROTECTION PRINCIPLES

The Business shall comply with the following 9 Data Protection Principles when processing personal data.

1. **Fairness and Transparency:** The Business must process personal data fairly and provide individuals with information about how and why their personal data is processed.

The Business must provide a privacy notice to each client, Personnel and Supplier to inform them of:

- the identity of the Business as data controller;

- the purposes for which their personal data are processed;
- the legal basis for processing;
- any legitimate interests pursued by the Business or a third party, if applicable;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the Business intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the relevant authority, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- the existence of the right to withdraw consent at any time, if applicable;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and
- the existence of Automated Decisions, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

For example, such privacy notice should be included in each client engagement letter or service agreement. If no engagement letter is issued, the privacy notice can be made available on the Business website or in other appropriate and easily accessible form. If the notice is published on the website, a conspicuous link to the website or privacy notice should be included in the Business email footer or other Notary stationery to bring the notice to the data subjects' attention.

Where a client provides personal data of third party data subjects to the Business, no notice will have to be provided to those third-party data subjects by the Business if such information must remain confidential subject to an obligation of professional secrecy. To the extent that no such obligation of

professional secrecy applies, the Business should place a contractual obligation on each client and Supplier to ensure that such notice is provided to those third-party data subjects on behalf of the Business.

2. **Lawful Processing:** The Business must only process personal data, including sensitive personal data, lawfully where it has a valid basis for the processing.

Generally, personal data must not be processed without a legal ground. In the context of the Business, personal data are typically processed based on:

processing is necessary for the performance of a contract (e.g. engagement letter) to which the data subject (e.g. the client) is party or to take steps at the request of the data subject prior to entering into a contract;

processing necessary for the legitimate interests pursued by a client or the Business, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This ground may apply to the processing of the personal data of any third-party data subjects whose personal data are provided by the client;

a legal obligation to which the Business is subject and where compliance with such obligation necessitates the processing of personal data by the Business;

- data subject's consent, where such consent is procured from the client; and
- other legal grounds.

3. **Purpose Limitation:** The Business must only collect personal data for a specific, explicit and legitimate purpose. Any subsequent processing should be compatible with that purpose, unless the Business has obtained the individual's consent, or the processing is otherwise permitted by law.

The Business will typically process:

- the personal data of its clients as required for the purposes of providing its professional services and the administration of its client relationships;
- the personal data of its Personnel as required for the administration of Personnel, if applicable;
- the personal data of its Suppliers as required for the administration of its Supplier relationships, if applicable; and
- the personal data of its clients, Personnel and Suppliers as is necessary to comply with its legal obligations.

The Business will generally not carry out any unsolicited electronic marketing, but to the extent it does, it will have to comply with the law.

4. **Data Minimisation:** The Business must only process personal data that is adequate, relevant and limited to what is necessary for the purpose for which it was collected.

The Business should place a contractual obligation on each client to ensure that only the minimum necessary personal data is provided in connection with the professional services sought.

Where a client provides personal data that appears excessive in connection with the professional services sought, the Business will return such personal data to the client and request that an adequate record of personal data is provided.

5. **Data Accuracy:** The Business must take reasonable steps to ensure personal data is accurate, complete, and kept up-to-date.

The Business should place a contractual obligation on each client to ensure that any personal data provided in connection with the professional services sought is accurate, complete and up to date.

The Business will endeavour to keep an accurate record of personal data in relation to its clients and Personnel.

6. **Individual Rights:** The Business must allow individuals to exercise their rights in relation to their personal data, including their rights of access, erasure, rectification, portability and objection.

The Business will ensure that all Individual Rights Requests are correctly identified and appropriately responded to, subject to any applicable exemptions.

7. **Storage Limitation:** The Business must only keep personal data for as long as it is needed for the purpose for which it was collected or for a further permitted purpose.

The Business will keep all records as long as required by applicable law or as may be necessary having regard to custom, practice or the nature of the documents concerned. For example, the Notaries Practice Rules 2014 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 6 years.

Save for personal data included in records which must kept for a prescribed period or preserved permanently in compliance with any legal obligations to which the Business is subject, such as the obligation explained above, personal data shall be kept for no longer than necessary for the relevant purpose. For example, any Personnel records should be kept for no longer than 12 months following the termination of employment or contract, unless a longer retention is required under applicable law.

8. **Data Security:** The Business must use appropriate security measures to protect personal data, including where third parties are processing personal data on our behalf.

The Business will adopt the following security measures:

*Physical security measures*

- ensure physical security of premises, e.g. locked office;
- keep documents in locked cabinets;
- reduce access privileges to only those needed;
- grant access to only such Personnel who need to have access in connection with their duties;
- dispose of documents using a confidential bin or through a cross cut shredder; and
- other appropriate physical security measures.

### *Organisational security measures*

- vet Personnel and Suppliers on a continuing basis;
- implement non-disclosure agreements prior to entering into formalised agreements;
- provide training to Personnel where appropriate;
- implement a strict ban on the use of personal email for work purposes; and
- other appropriate organisational security measures.

### *Technical security measures*

- firewalls which are properly configured and using the latest software;
- regular patch management and OS updates;
- real-time protection anti-virus, anti-malware and anti-spyware software;
- user access control management by, for example, the UAC functionality in Windows, adopting principle of least privileges;
- unique passwords of sufficient complexity and regular (but not too frequent) expiry;
- encryption of all portable devices ensuring appropriate protection of the key;
- data backup; and
- other appropriate technical security measures.

The Business will comply with *Policy: Appointing Suppliers*.

9. **Accountability:** We must take steps to comply with, and be able to demonstrate compliance, with the Data Protection Principles.

The Business will implement appropriate governance processes as set out in this Policy.

## **GOVERNANCE PROCESSES**

In order to ensure that the Data Protection Principles are implemented the Business shall adopt the following governance processes.

#### **A. Documented Policies**

In order to ensure compliance with Data Protection Principle 9 (Accountability), the Business shall comply with this Policy and implement such other data protection policies and establish internal governance processes from time to time as may be required in order to operate the Business in compliance with data protection laws.

#### **B. Assurance**

The Business will ensure, by way of training or otherwise, that Personnel carry out their tasks in a way that will ensure compliance with data protection laws. Each member of Personnel and each Supplier shall have access to this Policy and it shall have an obligation to comply with it.

Each Supplier will have to comply with data protection obligations in accordance with its service agreement including, where appropriate, a data processing agreement.

The Business shall periodically review this Policy and other policies to ensure that they continue to comply with the relevant legal requirements.

#### **C. Advice**

Where necessary the Business shall seek advice to ensure that its processes comply with data protection laws.

#### **D. Third Parties**

The Business shall comply with *Policy: Appointing Suppliers* in relation to appointing any third-party contractor or supplier who will process personal data on behalf of the Business.

#### **E. Data Protection Impact Assessments**

The Business shall implement a process so that any processing which is likely to result in a high risk to the rights and freedoms of individuals is subject to a documented Data Protection Impact Assessment (**DPIA**), to assess the risks associated with the proposed processing and identify any safeguards which should be put in place to mitigate those risks. The Business shall maintain a record of each DPIA.

## **F. Record-keeping**

The Business will implement a process to maintain an up-to-date documented record of its processing activities by way of adding relevant information in the Notary register or by other appropriate means.

This record should include a general description of the following:

### **Record keeping requirements**

#### **Suggested record**

- The purpose of the processing.
- Typically, in relation to Business transactions this will include processing to deliver client services;
- The categories of personal data and individuals to whom the data relates.
- a variety of mostly legal documents with copies of identity information relating to clients;
- The categories of recipients (if any), including both data controllers and data processors, and any transfers outside the European Economic Area (EEA).
- either the client or a third party to whom the client wished the documents to be sent after processing and such parties may often be located outside the EEA;
- Where possible, the envisaged retention period for the personal data.
- records will be retained in accordance with the Notaries Practice Rules; and
- Where possible, a general description of the technical and organisational security measures in place.
- the measures in place as set out at paragraph 8 above.

Although it is envisaged that the Business will act as data controller in the majority of cases, where the Business processes personal data on behalf of another person the Business will make sure to



maintain a record of its activities as a data processor and/or data controller. This record should include a general description of the following:

- The identity of the Business and contact details.
- The categories of processing carried out on behalf of the third party.
- Any transfers outside the EEA.
- Where possible, a general description of the technical and organisational security measures in place.

## **G. Privacy By Design**

When implementing a new processing activity, tool or functionality involved in the processing of personal data, the Business will ensure, by contractual means or otherwise, that such activity, tool or functionality is designed and built in a way that allows me to comply with the Data Protection Principles.

## **H. Complaint handling**

The Business shall implement a process to receive and handle enquiries and complaints from individuals and the supervisory authorities concerning the processing of personal data.

The Business shall ensure that all enquiries and complaints are dealt with in a timely manner, in compliance with any applicable statutory deadlines.

1.

## **APPENDIX: GLOSSARY**

**anonymous data**

Data which does not relate to an identified or identifiable individual, or personal data which has been rendered permanently anonymous in such a way that the individual is no longer identifiable (even if the data was combined with other data held by the Business Company).

### **Automated Decision**

A decision which produces legal effects, or similarly significantly affects an individual, and which is based solely on the automated processing (including profiling) of their personal data.

### **Business**

The business of providing notarial services.

### **controller**

A party which determines the purposes and means of the data processing.

### **data**

Any information which is recorded electronically or, where recorded in a manual format (e.g. on paper), is organised by reference to an individual.

### **data subject**

The individual to whom the personal data relates.

### **Individual Rights Request**

A request from a data subject in respect of their personal data, e.g. to access, erase, or rectify their personal data, or object to its processing.

### **personal data**

Any data relating to an identified or identifiable natural person. This can include (but is not limited to) names, addresses, email addresses, positions held, photographs, job applications, personnel files, occupational health records, opinions, and correspondence to and from an individual.

## **Personnel**

All employees of the Business at all levels, including, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors and external consultants.

## **processing**

Any operation performed on personal data, such as collection, recording, storage, retrieval, use, combining it with other data, transmission, disclosure or deletion.

## **processor**

A party processing personal data on behalf of a controller, under the controller's instructions.

## **pseudonymised data**

Personal data which can only be attributed to a specific individual by combining it with additional information (such as a key or other identifier), where the additional information is kept technically and logically separate from the pseudonymised data to avoid the individual being identified.

Pseudonymised data remains personal data.

## **Sensitive or special categories personal data**

Personal data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; biometric (e.g. fingerprints or facial recognition) or genetic information; or information about a person's health, sex life or sexual orientation, or relating to criminal convictions or offences (including allegations).

## **Supplier**

Any external vendor, supplier, consultant or similar third party engaged to provide services to the Business.

## DATA PROTECTION PRIVACY NOTICE

1. The business of **GS Notary Public Limited** of 44 Chiltern Way, Woodford Green IG8 0RQ ("**Business**", "**we**", "**us**", "**our**") is registered with the Information Commissioner's Office ("**ICO**") under number **ZA351211**.

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 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 paragraphs 8 & 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 as set out at paragraph 18, 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 **serving 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 clicking [here](#);
- 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. **complying with applicable law**, including Notary Practice Rules, guidelines and regulations or in response to a lawful request from a court or regulatory body.

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 (i).and

any other applicable legal grounds for processing from time to time.

## **Cookie statement**

### *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 placed on our website*

13. We 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](http://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 those 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 6 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](#).

**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 based on 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 must 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.