Appointing Suppliers Policy

INTRODUCTION

This Policy ("**Policy**") sets out the 9 Data Protection Principles which Sithira Pathberiya, Notary Public ("**Business**") commits to comply with when processing personal data in the course of its business of providing notarial services.

The steps which must be followed are:

Step 1: Establish whether the Supplier is a Data Controller or a Data Processor

Step 2: Comply with data protection law requirements in the procurement process

Step 3: Check whether personal data will be transferred outside the European Economic Area (EEA)

Step 4: Complete the self-assessment Checklist to ensure compliance with this Policy

This Policy does *not* apply if the Supplier's services do not involve the processing of personal data (for example where it is solely a contract for the purchase of goods, such as hardware).

STEP 1: IDENTIFY WHETHER THE SUPPLIER IS A DATA CONTROLLER OR A DATA PROCESSOR

Whenever it is proposed to appoint a Supplier to which this Policy applies, it is important to first identify whether the Supplier is a "Data Controller" or a "Data Processor".

- A **Data Controller** means a party that determines the purposes (that is, why the information is being processed) and means (that is, how the information is being processed) of processing. To identify this, one should ask: is the Supplier the controlling mind behind the proposed activity? Is the Supplier deciding what personal data will be collected and what it will be used for, or is it the Business? Often it is the person who "owns" the personal data. Broadly speaking, whoever "calls the shots" in relation to the personal data is likely to be a Data Controller. In the majority of cases the Supplier will likely be a Data Processor of the Business rather than a Data Controller. However, there may be situations where the Business appoints a Supplier who will be a Data Controller, as is shown in the examples below.
- A **Data Processor** means a party that processes the personal data on behalf of the Data Controller. To identify this, one should ask: is the Supplier carrying out the processing *only* because it has been instructed to do so by the Business? If so, the Supplier will usually be a Data Processor.

It is important to identify whether the Supplier is a Data Controller or Data Processor because:

- If a Supplier is a Data Controller it will be directly responsible for complying with EU data protection laws (for example ensuring that the processing of the personal data is fair and lawful, and enabling individuals to exercise their rights under data protection laws).
- If a Supplier is a Data Processor, it will still have some direct obligations under EU data protection laws. However, its primary obligations will be imposed under contract with the Data Controller, i.e. the Business. The Business will be legally responsible for all processing performed by its Data Processors, and so it is crucial that strict controls are placed on the Data Processor's actions.

EXAMPLES

SUPPLIER AS A DATA CONTROLLER (if any)

- A solicitor, accountant, notary or similar professional appointed to provide services to the Business.
- The Foreign Office or any other public authority will generally act under their official authority and will likely be a Data Controller.

- If the Business employs Personnel, it may engage a pensions provider for Personnel.

SUPPLIER AS A DATA PROCESSOR

- Where the Supplier is a data storage provider (e.g. NotarySafe service).
- An agent appointed to provide legalisation services (only if processing of personal data takes place, i.e. the documents are not provided in a sealed envelope and the Supplier can read them).
- A translation service provider.
- A confidential waste disposal service provider.
- An IT contractor with access to confidential information of the Business.
- If the Business employs Personnel, it may engage a payroll services provider to streamline the payroll process.

SUPPLIER NOT ENGAGED IN "PROCESSING"

- As mentioned above, this Policy does not apply if the Supplier's services do not involve the processing of personal data as set out in the examples below.
- Purchase of goods such as hardware, office supplies and other goods.
- Couriers are not considered processors as long as they do not access personal data, i.e. they are handed a sealed envelope which they must not open. They are a mere conduit between the sender and recipient.

If the Supplier will be acting as a Data Controller:

As mentioned above, it is less likely that a Supplier will be acting as Data Controller and the majority of Suppliers will be Data Processors. However, if the Supplier is indeed a Data Controller:

- The contract with the Supplier should contain standard terms for Data Controllers set out in Appendix 2.

  Please note that Data Controllers which are public authorities are less likely to accept a written agreement from the Business as they act under their official authority. In these cases, it may be reasonable for the Business to assume that the Data Controller will comply with its legal obligations even if no agreement is entered into. However, in some cases public authorities may still be considered Data Processors especially if they act outside their official authority and a written agreement (as per Steps 2 and 3) may be required. The Business should ensure that only such minimal possible personal data is shared with such public authorities as is required to carry out the relevant acts.

- Step 2 will not apply and Step 3, regarding data transfers, should be considered.

STEP 2: COMPLY WITH DATA PROTECTION LAW IN THE PROCUREMENT PROCESS.

Because the Business will be responsible for the actions of its Data Processors, there are certain steps which must be taken to protect the Business when appointing a Supplier who is a Data Processor.

In addition, when contracting with a Supplier who is a Data Processor, the Business is under a legal obligation to ensure certain **mandatory provisions** concerning personal data are included in the contract with the Data Processor. These provisions are reflected in the standard Data Processing Agreement.

The following table outlines the practical steps which should be taken during the procurement process to ensure that data protection legal obligations are met.

STEP	WHAT DOES THIS MEAN IN PRACTICE?
Understand the nature of the data processing	Identify the types and amounts of personal data which the Supplier will have access to. The Supplier should only have access to the minimum amount of personal data they need to provide the services. If the Supplier will have access to payment card data, the agreement will also need to address compliance with Payment Card Industry Data Security Standard (PCI DSS).
Conduct due diligence on the Supplier	Choose a Supplier providing sufficient guarantees regarding information security and handling of personal data. It should be ensured the Supplier is able to provide appropriate security protection for the data, taking into account the nature of the personal data and any risks involved (for example, the consequences of a security breach).
Take additional precautions with special categories of personal data or card payment data.	Pay particular attention to security specifications for the contract if it involves processing special categories of personal data.
Ensure the written contract contains or incorporates the data protection clauses	The contract with the Supplier must include specific data protection language, as this is a **legal requirement** under EU data protection laws. If the contract is on the Supplier's standard terms, it will still need to be ensured that the necessary data protection language is included in the contract.
Note any data transfers outside of the EEA	If any personal data will be transferred outside the EEA (including where the personal data can be accessed remotely from outside the EEA), steps must be taken to ensure that the transfer is lawful. See Step 3 below.
Anonymise, pseudonymise or aggregate personal data if possible	These safeguards should be considered to help eliminate data protection risks whenever possible.
Limit access to the personal data	The Supplier should have appropriate access controls so that only those involved in the delivery of the services can access the personal data, and access rights are limited to that necessary for each individual's role.
Ensure the Supplier can assist with individual rights requests	The data protection language in the contract must include an obligation on the Supplier to assist the Business to enable individuals to exercise their individual rights. These include rights to access, rectify and erase their personal data, and object to it being used for a particular purpose. The Supplier must ensure that it can respect these rights (e.g. by rectifying or erasing personal data), when requested to by the Business. The Supplier should also ensure that if it receives any requests in relation to personal data, these are promptly passed on to the Business.
Check the Supplier's subcontractors	Essentially, it should be ensured that all data processing terms will be 'flowed down' to any subcontractor.
Provide notice of the data sharing unless this has been done already	Ensure that the arrangement with the Supplier is covered by the privacy notice given to Personnel or clients, as applicable. If the arrangement is not adequately covered by the existing notice, consider how to inform them prior to providing their personal data to the Supplier.
Business monitors the Supplier's compliance throughout the appointment	Ensure there are reasonable steps in place which allow a Business to monitor the Supplier's performance with its security and processing obligations. For example, the Business may check the Supplier's website and look out for any relevant press releases from time to time and regularly (depending on level of engagement and associated risks) ask the Data Processor (e.g. pursuant to the Data Processing Agreement) for information such as a confirmation of the information security measures that the Data Processor has in place from time to time.

Establish what will happen to the personal data at the end of the relationship	If there is no longer a need to keep the personal data, because of the termination of the service relationship or because the law no longer requires it, it should be returned to the Business. Make sure the contract terms provide for the return of the personal data to the Business or purging upon request of the Business.

STEP 3: CHECK IF PERSONAL DATA WILL BE TRANSFERRED OUTSIDE THE EEA

This Step 3 should be completed whether the Supplier will be acting as a Data Controller or a Data Processor.

In considering whether to appoint a Supplier, the following should be established:

- whether the Supplier is, itself, located outside the EEA; or
- whether the Supplier may *subsequently* transfer personal data outside the EEA (for example to the Supplier's subsidiaries or subcontractors).

A 'transfer' of personal data includes the following:

- allowing personal data **stored** in the EEA to be **accessed remotely** from a country outside the EEA (e.g. the US);
- relocating a database outside the EEA; or
- sending a data set (for example an Excel file) as an attachment to an email to a recipient outside the EEA.

Subject to the exceptions set out below, personal data should not be transferred from an EEA country to a non-EEA country unless there are means of providing appropriate safeguards for that personal data.

A small number of countries (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay) have been legally recognised to provide an adequate level of protection and personal data can therefore be transferred from the EEA to those countries. The list of "adequate" countries can be found on the Commission's website here.

The US is also regarded as "adequate" if the US recipient (whether the Supplier or a subcontractor) is certified with the EU-US Privacy Shield, and their certification covers the type of personal data which will be transferred. If the Supplier wants to rely on Privacy Shield, the recipient's certification should be checked on the online list. If the Supplier will be relying on Privacy Shield, ensure it is subject to an obligation to maintain its Privacy Shield status for the duration of the agreement (or ensure the relevant US recipient does), and is obliged to enter into an alternative transfer solution if Privacy Shield is no longer valid.

For countries outside the EEA and not listed above an alternative solution has to be adopted before personal data can be transferred. The most relevant to the Business is likely to be requiring the non-EEA recipient to sign up to an approved set of international data transfer clauses, known as the 'EU Model Clauses'. Which version of the Clauses should be used depends on whether the Supplier is acting as a Controller or a Processor. The EU Model Clauses should not be amended by the parties. The Appendices will need to be completed prior to execution.

Summary of the contractual arrangements which must be in place:

Country in which personal data will be hosted in, or will be accessible from	**How to regulate processing by the Supplier**	**How to regulate transfers outside the EEA**
'Adequate' countries (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay)	Use the standard Data Processing Agreement	N/A as the countries offer 'adequate protection'

Non-adequate countries (e.g. Australia, India, China, or US companies not registered with the Privacy Shield)	Use the standard Data Processing Agreement	Execute the applicable EU Model Clauses
US Companies who are certified with the EU-US Privacy Shield, and their certification covers the type of personal data being transferred	Use the standard Data Processing Agreement	Ensure the Supplier is obliged to remain certified with the Privacy Shield throughout the term of appointment, and to put in place an alternative arrangement if Privacy Shield is no longer valid

Exceptions

In some circumstances transfers may be made without ensuring appropriate safeguards for the transferred personal data, as explained above. These exceptions will mostly concern transfers instructed by the client rather than transfers to a Supplier of the Business.

Explicit consent from data subject.	This will only apply where all personal data in the document to be transferred outside the EEA is the personal data of the client and no third party (unless such third party also consented). Consent has to be freely given, unambiguous, informed and confirmed by affirmative action or statement of the data subject. A record of the consent must be retained together with the assessment of possible risks of the transfer and the appropriate safeguards put in place in relation to the transfer.
Transfer is necessary for the performance of contract	This will apply only to contracts between the Business and the data subject or another party on the data subject's request. This may apply, for example, where the client engages the Business to procure notarisation by foreign notaries. In such cases, the Business should obtain a warranty from the client to the effect that the client has obtained explicit and demonstrable consent from each other data subject whose personal data is included in the document which is subject to the transfer. This exception will also likely apply to transfers to foreign public authorities.
Transfer is necessary for important reasons of public interest recognised by law.	This will apply in very limited circumstances, such as in the case of the UK's substantial public interest in detecting and preventing crime.
Information in public registers.	You can transfer overseas part of the personal data on a public register, as long as the person you transfer to complies with any restrictions on access to or use of the information in the register.
Transfer is necessary in connection with legal proceedings, legal advice or defending legal rights.	This may apply, for example, where notarised documents are forwarded to a third party law firm in connection with legal proceedings or legal advice.

These are the main exceptions that are likely to apply. However, in some circumstances further exceptions may apply.

STEP 4: SELF-ASSESSMENT CHECKLIST FOR COMPLIANCE WITH THIS PROCEDURE

To ensure compliance with the requirements of this Policy, the self-assessment checklist in Appendix 1 should be completed.

Last updated January 2024

APPENDIX 1

SUPPLIER APPOINTMENT SELF-ASSESSMENT CHECKLIST

This checklist will help you determine whether this Policy has been complied with. If any of your answers is "No", further information from the Supplier or independent legal advice should be sought.

HAVE ALL ACTIONS BEEN TAKEN TO ENSURE THE COMPLIANCE OF THE NEW SUPPLIER APPOINTMENT?	**COMPLETED**
I have identified what types of personal data will be disclosed to the Supplier.	
I have identified whether the Supplier will act as a Data Controller or a Data Processor in this processing.	
I have ensured that our contract with the Supplier addresses data protection compliance in lieu of its role in the processing.	
I have ensured that the Supplier requires personal data only as much as needed to achieve the purpose for which the Supplier is appointed and not more.	
I have considered with the Supplier whether providing pseudonymised, anonymised or aggregated personal data is adequate for the processing.	
For the personal data which is sensitive personal data I have ensured that the Supplier will take additional security measures to protect this personal data.	
I have taken steps to ensure that the Supplier only allows those within the Supplier with a genuine 'need-to-know' to have access to the personal data.	
I have taken steps to ensure that the Supplier will keep logs or records regarding processing of the personal data, including who accessed the data, when, whether data was changed, deleted, etc.	
I have taken steps to ensure that the Supplier will store the personal data only as long as needed for the purpose and no longer.	
I have taken steps to ensure that all personal data will be purged, erased or returned at the end of the appointment.	
I understand what (if any) other parties will be involved in providing the services and have ensured that the data processing requirements will be flowed down to the subcontractor.	
The processing requires the personal data to be accessible outside the EEA. I have put a transfer solution in place (see Step 3).	
I have put in place an internal process to monitor the Supplier's compliance throughout the appointment.	
I have taken steps to ensure that the relevant individuals have been / will be informed that their personal data will be used for this appointment and disclosed to a Supplier.	

APPENDIX 2

STANDARD DATA PROTECTION TERMS: DATA CONTROLLERS

[INSTRUCTIONS FOR USE: This clause is intended for inclusion in a services agreement where a Supplier will be acting as a Data Controller (i.e. it determines the purposes and means of the processing of the personal data from the Business).

Remove all Drafting Notes prior to sharing with the Supplier]

"Data Protection Legislation"	shall mean all applicable laws relating to data protection and privacy including (without limitation) the EU Data Protection Directive (95/46/EC) as implemented in each jurisdiction, the EU General Data Protection Regulation (2016/679), the EU Privacy and Electronic Communications Directive 2002/58/EC as implemented in each jurisdiction, and any amending or replacement legislation from time to time;
"Customer personal data"	shall mean all personal data (as defined in the Data Protection Legislation) controlled by Customer which is processed by the Supplier in connection with the Services;

[Ensure the Services Agreement contains defined terms for "Agreement", "Services", "Supplier" (which must include all EU affiliates)]

DATA PROTECTION

1. In this clause [1], the terms "personal data", "process", "data controller" and "data processor" shall have the meanings set out in the Data Protection Legislation.
2. The Supplier acknowledges that it shall be acting as an independent data controller in respect of Customer personal data.
3. Without prejudice to clause [1.2], if circumstances arise whereby the Supplier is acting as a data processor on Customer's behalf the Supplier shall promptly, on request by Customer, execute written contractual commitments which meet the requirements of the Data Protection Legislation. Until such written commitments can be put in place, this clause [1] shall be interpreted to give the closest possible effect to the requirements of the Data Protection Legislation.
4. The Supplier shall comply with its obligations under the Data Protection Legislation in respect of Customer personal data. Without prejudice to the foregoing, the Supplier shall not process Customer personal data in a manner that will or is likely to result in Customer breaching its obligations under the Data Protection Legislation.
5. The Supplier shall only process Customer personal data for the purposes of performing its obligations under this Agreement and for which it was disclosed by Customer to the Supplier.

   [The formulation below should be used if the transfer of data outside the EEA is not contemplated from the outset. Note that if this wording is used, there is no need to include clause [1.6] and [1.7]

6. The Supplier shall not process Customer personal data outside the European Economic Area ("**EEA**") (including by way of remote access) without the prior written consent of Customer.]

   [OR]

   [Alternative clause 1.6 which should be used (in combination with clause 1.6 and 1.7) if there will be a transfer of data from the outset:

   Customer hereby consents to Customer personal data being processed outside the EEA, subject to the Supplier's continued compliance with clause [1.6] and clause [1.7] throughout the duration of this Agreement.]

   [Clause 1.6 and 1.7 are only required if data will be transferred from the outset. Use the formulation below if the service provider is based outside the EEA but is not a US-company registered with Privacy Shield:

7. To the extent that Customer personal data is processed outside the EEA, the terms of the transfer shall be governed by the EU Standard Contractual Clauses for the transfer of personal data to third countries (controller to controller transfers) attached as [**Appendix 1**], which are hereby incorporated into this Agreement.]

   [The following clause should be included where the Supplier is in the US and certified with Privacy Shield, and its certification covers the data transferred. Note that this clause can still be used if the personal data will subsequently be transferred to a third country by the Supplier, provided the initial transfer is to the US:

   The Supplier hereby warrants and represents that as of the Effective Date it is registered with the EU-US Privacy Shield, approved by the European Commission (Decision of 12th July 2016) ("Privacy Shield"). The Supplier further agrees:

   (a) to maintain its adherence to the Privacy Shield throughout the duration of this Agreement; and
   (b) to immediately inform Customer if at any time the Supplier ceases to be Privacy Shield certified during the term of this Agreement, for whatever reason.]

8. If, for whatever reason, the transfer of Customer personal data under Clause [1.6] ceases to be lawful, the Supplier shall either:

   (a) with Customer's consent, implement an alternative lawful transfer mechanism; or
   (b) allow Customer to terminate the Agreement at no additional cost to Customer.]

PLEASE INCLUDE APPENDIX 1 INCLUDING THE STANDARD CONTRACTUAL CLAUSES