CARRUTHERS CURDIE STURROCK & CO.

DATA PROTECTION POLICY

1 Introduction

1.1 Carruthers Curdie Sturrock & Co. (CCS-Solicitors) is fully committed to complying with the requirements of the Data Protection Act 1998 (as amended) and the General Data Protection Regulation (EU) 2016/679 (the Data Protection Legislation).

1.2 CCS-Solicitors recognises that the Data Protection Legislation is important in relation to protecting the rights of individuals on whom CCS-Solicitors keeps and uses personal data, whether electronically or within structured paper filing systems.

1.3 CCS-Solicitors will therefore follow procedures that aim to ensure that all employees, agents, consultants, partners or other persons involved in the work of CCS-Solicitors and who have access to any personal data held by or on behalf of CCS-Solicitors, are fully aware of and abide by their duties and responsibilities under the Data Protection Legislation and assist CCS-Solicitors in doing so.

2 Statement of Policy

2.1 In order to operate efficiently and fulfil its functions, CCS-Solicitors must collect and use data about people with whom we work in order to provide our services. These may include: our clients; beneficiaries; individuals on the other side of transactions; and current, past and prospective employees.

2.2 In addition, CCS-Solicitors may be required to collect and use certain types of data for legal compliance purposes. This personal data must be handled properly, irrespective of how it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

2.3 CCS-Solicitors regards the lawful and correct treatment of personal data as very important to its successful operations and to maintaining confidence between CCS-Solicitors and the full range of stakeholders in our work. CCS-Solicitors will ensure that it treats personal data lawfully and correctly and in accordance with the Data Protection Legislation.

3 Glossary of Key Terms

3.1 The following is a glossary of key terms in the Data Protection Legislation:

3.1.1 Information Commissioner's Office (the ICO) – the ICO is the body responsible for enforcing and monitoring compliance with the Data Protection Legislation;

3.1.2 Controller – the organisation that determines the purposes for which and manner in which personal data is used, in our case, CCS-Solicitors;

3.1.3 Data subject – a living individual who is the subject of personal data, for example, client, employee, beneficiaries, parties on the other side of

transactions, Marr Trust scholarship / beneficiary recipients, members of the Oddfellows Friendly Society, etc;

3.1.4 Personal data – any information relating to an identifiable person who can be directly or indirectly identified from that information, in particular by reference to an identifier;

3.1.5 Special category personal data is defined as personal data revealing a data subject's:

3.1.5.1 racial or ethnic origin;

3.1.5.2 political opinions;

3.1.5.3 religious or philosophical beliefs;

3.1.5.4 trade union membership;

3.1.5.5 health;

3.1.5.6 sex life or sexual orientation; and

3.1.5.7 genetic or biometric data where processed for the purpose of uniquely identifying a data subject; and

3.1.6 Processing – any operation performed on personal data, including obtaining, recording, storing, using, disclosing and deleting.

4 Principles of Data Protection

4.1 The Data Protection Legislation stipulates that anyone processing personal data must comply with the principles of good practice (the Principles).

4.2 The Principles require that personal data shall be:

4.2.1 processed lawfully, fairly and in a transparent manner;

4.2.2 obtained only for specific, explicit and legitimate purposes and not processed for any other purpose that is incompatible with those purposes;

4.2.3 adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed;

4.2.4 accurate and where necessary, kept up to date;

4.2.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which it is processed; and

4.2.6 kept secure by means of appropriate technical and organisational safeguards.

5 Handling of Personal / Special Category Personal data

5.1 CCS-Solicitors will, through appropriate management and the use of strict criteria and controls:

5.1.1 observe fully the conditions regarding the fair collection and use of personal data;

5.1.2 meet its legal obligations to specify the purpose(s) for which personal data is used;

5.1.3 collect and process appropriate personal data and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;

5.1.4 ensure the quality of personal data used;

5.1.5 apply strict checks to determine the length of time special data is held and either archive or destroy it when it is no longer relevant or required;

5.1.6 take appropriate technical and organisational security measures to safeguard personal data;

5.1.7 ensure that personal data is not transferred outwith the EU without suitable safeguards; and

5.1.8 ensure that the rights of people about whom the data is held are respected and can be fully exercised by them under the Data Protection Legislation and against CCS-Solicitors.

5.2 CCS-Solicitors will also ensure that:

5.2.1 there is someone with specific responsibility for data protection within CCS-Solicitors;

5.2.2 everyone within CCS-Solicitors who is managing and handling personal data understands that CCS-Solicitors is legally responsible for following good data protection practice and complying with the Data Protection Legislation;

5.2.3 everyone managing and handling personal data within CCS-Solicitors is appropriately trained to do so;

5.2.4 everyone managing and handling personal data within CCS-Solicitors is appropriately supervised;

5.2.5 queries and complaints about handling personal data are promptly and courteously dealt with;

5.2.6 methods of and performance in relation to handling personal data are regularly assessed and evaluated; and

5.2.7 data processing by third parties on behalf of CCS-Solicitors is carried out under a written agreement.

5.3 All staff within CCS-Solicitors will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and, in particular, will ensure that:

5.3.1 paper files and other records or documents containing personal / special category personal data are kept in a secure environment;

5.3.2 access to personal data is only provided on a "need to know" basis to those staff who require access for the purposes of fulfilling the requirements of their role within CCS-Solicitors;

5.3.3 appropriate technical measures, including internet security, anti-virus software and firewalls, are installed and kept up-to-date;

5.3.4 personal data held on computer systems is protected by the use of secure passwords, which have forced changes periodically and mandate strong password security; and

5.3.5 individual passwords should be such that they are not easily compromised.

5.4 Further guidance for staff in handling personal data is contained within the Appendix to this Policy.

5.5 All contractors, consultants, partners or other associates or agents of CCS-Solicitors must (as a minimum):

5.5.1 only act on the written instructions of CCS-Solicitors (unless required by law to act without such instructions);

5.5.2 ensure that people processing personal data on behalf of CCS-Solicitors are subject to a duty of confidence;

5.5.3 only engage a sub-contractor to process personal data on behalf of CCS-Solicitors with the prior consent of CCS-Solicitors and a written contract;

5.5.4 assist CCS-Solicitors in responding to requests from data subjects seeking to exercise their rights under the Data Protection Legislation;

5.5.5 assist CCS-Solicitors in meeting its obligations under the Data Protection Legislation in relation to security of processing, the notification of personal data breaches and data protection impact assessments where applicable;

5.5.6 delete or return all personal data to CCS-Solicitors as requested at the end of the contract;

5.5.7 allow data protection audits and inspections by CCS-Solicitors of personal data held on its behalf (if requested) to ensure that both parties are meeting their requirements under the Data Protection Legislation and tell CCS-Solicitors immediately if asked to do something that infringes the Data Protection Legislation; and

5.5.8 indemnify CCS-Solicitors against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

5.6 All contractors who are users of personal data supplied by CCS-Solicitors will be required to confirm that they will abide by the requirements of the Data Protection Legislation with regard to data supplied.

6 Basis and purposes for processing personal data

6.1 Before any personal data is processed by CCS-Solicitors for the first time, CCS-Solicitors will:

6.1.1 review the purposes of the particular processing activity and select the most appropriate lawful basis under the Data Protection Legislation. The lawful bases most commonly used by CCS-Solicitors are that:

6.1.1.1 the individual has consented – this is only appropriate where it is not a precondition of a service or another lawful basis applies and does not apply to staff personal data;

6.1.1.2 the processing is necessary for performance of or to take steps to enter into a contract with the individual – this will apply to our clients, staff and anyone requesting services from CCS-Solicitors;

6.1.1.3 the processing is necessary to comply with a legal obligation – CCS-Solicitors needs to process certain personal data under law, such as client personal data for The Law Society of Scotland's regulatory requirement or staff personal data for HMRC reporting purposes; or

6.1.1.4 the processing is necessary for CCS-Solicitors' or a third party's legitimate interests – provided that the legitimate interests are not overridden by the interests of the data subject;

6.1.2 where special category personal data is involved in the processing activity, identify the most appropriate special condition for processing in addition to a lawful basis above. The special conditions most commonly used by CCS-Solicitors are that:

6.1.2.1 the individual has explicitly consented – this is only appropriate where it is not a precondition of a service or another lawful basis applies and does not apply to staff personal data;

6.1.2.2 the processing is necessary for CCS-Solicitors to perform our obligations or exercise rights under employment law – this would apply to staff personal data, for example, to maintain attendance and performance records; or

6.1.2.3 the processing is necessary for CCS-Solicitors to establish, exercise or defend legal claims;

6.1.3 document CCS-Solicitors' decision as to which lawful basis applies, to help demonstrate compliance with the Principles; and

6.1.4 include information about the purposes, lawful basis and special condition (if applicable) of the processing within the relevant privacy notice provided to individuals.

6.2 CCS-Solicitors will review the procedures above every five years.

7 Documentation and records

7.1 CCS-Solicitors keeps written records of processing activities, including:

7.1.1 the name and details of CCS-Solicitors;

7.1.2 the purposes of the processing of personal data by CCS-Solicitors;

7.1.3 a description of the categories of individuals and categories of personal data processed by CCS-Solicitors;

7.1.4 categories of recipients of personal data with whom CCS-Solicitors shares personal data;

7.1.5 where relevant, details of transfers to countries outwith the EU, including documentation of the transfer mechanism safeguards in place;

7.1.6 details of how long CCS-Solicitors keeps personal data, the Data Retention Policy; and

7.1.7 a description of technical and organisational security measures put in place to keep personal data secure.

7.2 CCS-Solicitors will issue privacy notices from time to time to ensure that individuals understand how their personal data is collected, used, stored, shared and deleted by CCS-Solicitors.

8 Rights of data subjects

8.1 Data subjects have the following rights in relation to their personal data:

8.1.1 to be informed about how, why and on what basis that information is processed – as contained within CCS-Solicitors' privacy notices;

8.1.2 to obtain confirmation that their personal data is being processed by CCS-Solicitors and to obtain access to it and certain other information, by making a subject access request;

8.1.3 to have personal data corrected if it is inaccurate or incomplete;

8.1.4 to have personal data erased if it is no longer necessary for the purpose for which it was originally collected / processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as the "right to be forgotten");

8.1.5 to restrict the processing of personal data where the accuracy of the data is contested, or the processing is unlawful (but the individual does not want the personal data to be erased), or where CCS-Solicitors no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim; and

8.1.6 to restrict the processing of personal data temporarily where the individual does not think it is accurate (and CCS-Solicitors is verifying whether it is accurate), or where the individual has objected to the processing (and CCS-Solicitors is considering whether its legitimate grounds override the data subject's interests).

8.2 Individuals wishing to make a request to exercise their rights should make the request in writing to the Data Protection Compliance Partner.

8.3 Where staff receive a request from an individual that relates to their personal data and they are not authorised to handle such a request, staff must immediately notify the Data Protection Compliance Partner of the request. The Data Protection Legislation only gives CCS-Solicitors one month to respond to requests so staff should not delay in notifying the Data Protection Compliance Partner of any request.

9 Retention and disposal of personal data

9.1 CCS-Solicitors will retain personal data contained within client files in accordance with the Law Society of Scotland's guidelines:

(https://www.lawscot.org.uk/members/rules-and-guidance/rules-and-guidance/section-e/division-b/guidance/the-ownership-and-destruction-of-files/).

9.2 Staff should read this Policy in conjunction with the Data Retention Policy.

10 Data breaches

10.1 A data breach may take many different forms, for example:

10.1.1 loss or theft of data or equipment on which personal data is stored;

10.1.2 unauthorised access to or use of personal data either by a member of staff or third party;

10.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

10.1.4 human error, such as accidental deletion or alteration of data;

10.1.5 unforeseen circumstances, such as a fire or flood;

10.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

10.1.7 'blagging' offences, where information is obtained by deceiving CCS-Solicitors.

10.2 CCS-Solicitors will:

10.2.1 make the required report of a data breach to the ICO without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

10.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

10.3 It is important that staff report any suspected or actual data breach to the Data Protection Compliance Partner immediately. The Data Protection Compliance Partner will be responsible for recording and reporting data breaches.

11 Implementation of this Policy

11.1 It is essential that CCS-Solicitors complies with the Data Protection Legislation and does not obtain, process or store personal data for purposes other than those that have been notified to the ICO. To ensure compliance with the Data Protection Legislation, staff must be aware that this relates to data held on current, former or prospective: clients; applications for employment; employees; pension administration; payroll; and supplier administration.

11.2 This section of this Policy defines the responsibilities for data protection within CCS-Solicitors:

11.2.1 the Data Protection Compliance Partner has overall responsibility for data protection within CCS-Solicitors, and for ensuring:

11.2.1.1 that the notification to the ICO, and entry in the data protection register, is accurate and up-to-date;

11.2.1.2 the provision of data protection training, advice and support for staff within CCS-Solicitors to ensure full compliance with the Data Protection Legislation;

11.2.1.3 the development of best practice guidelines;

11.2.1.4 compliance checks to ensure adherence to the Data Protection Legislation;

11.2.1.5 any complaints in relation to alleged breach of the Data Protection Legislation and this Policy are handled appropriately; and

11.2.1.6 requests from individuals to access personal data CCS-Solicitors holds on them are responded to in accordance with the Data Protection Legislation; and

11.2.2 all staff have a responsibility to fully comply with the requirements of the Data Protection Legislation and this Policy. When involved in disclosing personal data to a third party, staff will confirm why the data is necessary, what it will be used for and who will have access to it once it has been disclosed.

11.3 A copy of this Policy will be given to all new members of staff, contractors, other stakeholders or interested third parties. Existing staff and any relevant stakeholder will be advised of this Policy, which will be posted on our server. All staff and stakeholders are to be familiar with and comply with this Policy at all times.

12 Complaints

12.1 Where any data subject feels that CCS-Solicitors has:

12.1.1 misused their personal data;

12.1.2 refused to allow access to data;

12.1.3 refused to amend alleged inaccuracies; or

12.1.4 otherwise breached the Data Protection Legislation in relation to their personal data or data protection rights,

they can complain to CCS-Solicitors.

12.2 All complaints will be handled in line promptly and courteously.

12.3 Data subjects may also raise complaints with the ICO.

13 Breaches of this Policy

13.1 A breach of the Data Protection Legislation could be a criminal offence and CCS-Solicitors or any individual employee who is involved could be liable for significant penalties.

13.2 Any allegations against a member of staff will be investigated thoroughly by CCS-Solicitors.

13.3 In the case of any breach of this Policy by consultants, contractors, agents or partners, CCS-Solicitors will consider the level of breach and any recurrence to inform its decision on whether to terminate the contract.

14 Training

Data protection training and awareness is essential to ensure our staff are fully aware of their responsibilities in the management and processing of personal data, which will ensure compliance with the Policy.

15 Risk Management and Audit

15.1 There are potential financial penalties and compensation payments due following on from a failure to comply with the Data Protection Legislation.

15.2 CCS-Solicitors aims to mitigate the risk of failure to comply through the provision of training to staff on data protection issues. CCS-Solicitors will review this Policy and the associated procedures on a regular basis to ensure that they meet all legislative and regulatory requirements and best practice guidance. In addition, an annual audit and review of personal data held by CCS-Solicitors will be carried out to ensure ongoing compliance with the provisions of the Data Protection Legislation.

15.3 Internal audit procedures will form an important part of establishing and sustaining good data protection practices. CCS-Solicitors will review the data it processes and collects and assess this against the Principles.

15.4 We will undertake self assessment to periodically check our compliance with the Data Protection Legislation; this Policy, regulatory and good practice guidance; our registration with the ICO; and our working practices in the collection, processing and storage of personal data.

15.5 Data protection issues will continue to be considered as part of CCS-Solicitors' risk management strategy.

16 Policy Review

16.1 As a strategic document, this Policy will be reviewed every three years. The next review will therefore take place in April 2023 or earlier to take account of:

16.1.1 legislative, regulatory and good practice requirements;

16.1.2 CCS-Solicitors' performance; or

16.1.3 the views of any stakeholder in the use of personal data.

Appendix

Staff Guidance

1 The Data Protection Legislation

1.1 The Data Protection Legislation establishes the principles of good Data Protection practice.

1.2 These principles are that personal data must be:

1.2.1 processed lawfully, fairly and in a transparent manner;

1.2.2 obtained only for specific, explicit and legitimate purposes and not processed for any other purpose that is incompatible with those purposes;

1.2.3 adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed;

1.2.4 accurate and where necessary, kept up to date;

1.2.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which it is processed; and

1.2.6 kept secure by means of appropriate technical and organisational safeguards.

1.3 The Data Protection Legislation applies to almost every conceivable use of personal data, from the moment the data is obtained to the method of recording, retrieving, disclosing and destroying it.

1.4 The Principles apply to both personal data held on IT systems and structured paper files and cover both facts and opinions about the individual.

1.5 This guidance is intended to help you handle data correctly. If you have any queries or concerns, please speak to the Data Protection Compliance Partner.

2 Keeping personal data secure

2.1 Staff must

2.1.1 keep passwords secure – change them regularly, do not share them with others;

2.1.2 lock / log off your computer when away from your desk;

2.1.3 dispose of confidential paper waste securely;

2.1.4 take care when opening emails and attachments from unknown sources to prevent virus attacks;

2.1.5 keep your desk clear, storing hard copy personal data securely when it is not being used;

2.1.6 sign visitors in and out of the premises;

2.1.7 position your computer screen away from windows or where visitors can see them; and

2.1.8 encrypt personal data which is being taken out of the office – for example, on a laptop or USB memory stick.

3 Meeting the reasonable expectations of clients, other customers and employees

3.1 Staff must:

3.1.1 collect only the personal data you need for a particular business purpose;

3.1.2 obtain consent to hold personal data;

3.1.3 update records promptly to reflect changes of name and address;

3.1.4 delete personal data that is not relevant or no longer required;

3.1.5 do not release personal data without consent or unless otherwise lawful under the Data Protection Legislation; and

3.1.6 advise your line manager of any potential data breaches.

4 Disclosing personal data over the telephone

4.1 Do not disclose personal data over the telephone without authenticating the identity of the caller.

4.2 If it is an individual claiming to be a client, you should run through some standard security queries regarding the client, including:

4.2.1 full name and address including postcode;

4.2.2 recent instructions (if applicable);

4.2.3 date of birth (if data held); and

4.2.4 password (if data held).

5 Email

5.1 Email is not secure and should not routinely be used for special category personal data, private or confidential data.

5.2 Staff who wish to send personal or special category personal data by email will need to protect the file by using a password to protect the personal data and by

marking the email subject matter with "Private & Confidential". Staff training can be provided on request.

5.3 Emails referring to an individual or organisation can be requested as part of a data request and staff should ensure that content is at all times accurate and reflective of Company's policy and that the tone is appropriate and professional.

6 What data should I record and hold?

6.1 The Data Protection Legislation states that the data you hold should be adequate, relevant, not excessive and accurate for the purposes for which it is held.

6.2 Our objective is to keep data to a minimum but enough to enable you to fulfil the function you are completing.

6.3 If it is necessary to hold additional data about certain individuals, such data should only be collected and recorded in those cases.

6.4 It is not acceptable to hold data on the basis that it might possibly be useful in the future without a view of how it will be used.

6.5 Data is inaccurate if it's incorrect or misleading as to any matter of fact. Ensure that your data is accurate and kept up to date. Data is more likely to be challenged for accuracy if it contains subjective or irrelevant comments. Use every opportunity to check that your files are up to date and accurate e.g each time you access an individual's data.

7 Requests from individuals under the Data Protection Legislation

7.1 CCS-Solicitors must comply with requests from individuals relating to their personal data promptly and within one month from the receipt of the request. We are able to extend this period by two months for complex or numerous requests, provided we notify the individual within one month of receiving the request of such extension.

7.2 An individual has a legal right to request access to any personal data we hold about them. The individual is entitled to know:

7.2.1 the type of personal data we hold about them;

7.2.2 the purposes for which we hold the personal data;

7.2.3 who the personal data may be disclosed to;

7.2.4 where we obtained the personal data from;

7.2.5 where possible, the envisaged period for retaining the personal data or criteria used to determine that period;

7.2.6 the existence of their rights under the Data Protection Legislation; and

7.2.7 the right to complain to the ICO.

7.3 They are also entitled to a copy of any data we hold about them with any unintelligible terms explained.

7.4 Remember that we hold personal data in a number of different formats, including paper files and on IT systems.

7.5 You do not have to disclose data if it involves sharing personal data about another individual, unless that person has given their consent or it is reasonable to proceed to disclose their personal data without their consent. If the personal data relating to that other person could be redacted then this is acceptable, provided that the other text does not give data which could result in the identification of that person e.g. in a complaint (unless the complainant has given you consent) you must not disclose their details.

7.6 An individual has a right to have their personal data corrected if it is inaccurate or incomplete. If we consider that their personal data does need to be rectified, we must rectify the personal data that we hold and notify any third parties who have received the relevant personal data.

7.7 An individual has a right to have their personal data deleted where:

7.7.1 the personal data is no longer necessary for the purposes it was originally collected / processed;

7.7.2 when the basis for processing the individual's personal data is consent and they withdraw their consent;

7.7.3 when the individual objects to the processing of their personal data and we do not have an overriding legitimate interest to continue the processing;

7.7.4 the personal data was unlawfully processed – i.e. in breach of the Data Protection Legislation; and

7.7.5 the personal data has to be deleted in order to comply with a legal obligation.

7.8 There are certain circumstances when we can refuse a request for erasure, such as when the personal data is processed for the following reasons:

7.8.1 to exercise the right of freedom of expression and information;

7.8.2 to comply with a legal obligation to perform a public interest task or exercise official authority;

7.8.3 for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or

7.8.4 to establish, exercise or defend legal claims.

7.9 An individual has a right to ask us to restrict the processing of personal data where:

7.9.1 when an individual claims that the personal data is inaccurate, the processing of that personal data should be restricted until the accuracy of it is verified;

7.9.2 when we are considering if our legitimate interests override those of the individual where the individual has objected to the processing of their personal data;

7.9.3 when we are processing is unlawful and the individual requests restriction of the processing of their personal data rather than erasure; and

7.9.4 when we no longer need the personal data but the individual requires their personal data to establish, exercise or defend a legal claim.

7.10 Individuals have the right to object to our processing of their personal data where it is used for:

7.10.1 legitimate interests or to perform a task in the public interest / exercise of official authority:

7.10.1.1 individuals can object for reasons relating to their particular situation; and

7.10.1.2 we must stop processing the personal data unless our legitimate interests override those of the individual or the processing is to establish, exercise or defend legal claims;

7.10.2 direct marketing: as soon as we receive an objection to direct marketing activities, we must stop processing the individual's personal data for direct marketing purposes immediately; and

7.10.3 scientific / historic research and statistics:

7.10.3.1 individuals can object for reasons relating to their particular situation; and

7.10.3.2 we are not required to comply with an objection where the processing of personal data is necessary for the performance of a public interest task.

7.11 An individual has a right to request their personal data from us and reuse it for their own purpose. This right only applies to personal data provided to us by an individual, where we process the personal data based on the individual's consent or in order to perform a contract, and the processing is carried out by automated means (i.e. inputted into any of our IT systems).

7.12 The Data Protection Compliance Partner is responsible for responding to requests from individuals to access their personal data and all other requests from individuals under the Data Protection

8 What happens if I breach the Data Protection Legislation?

8.1 Breaches of the Data Protection Legislation may result in disciplinary action.

8.2 It is essential that you report any breach or potential breach of the Data Protection Legislation to your line manager immediately. This will allow CCS-Solicitors to assess and mitigate the risks and implications of the breach.

9 Support & guidance

If any staff member is unsure about the disclosure of data or any other matter they should seek support and guidance from the Data Protection Compliance Partner in the first instance.