

Scott + Scott UK LLP

Client Data Protection Policy

1. Introduction

- 1.1 In the course of our acting for you, we may receive information relating to you, your directors, shareholders, beneficial owners, employees, agents, associates and family members. In this Policy, we refer to this information as “personal information”, which is any information relating to an identified or identifiable individual.
- 1.2 This Policy sets out the basis on which we will process this personal information. Please read the Policy carefully to understand our practices regarding personal information and how we will use it. It also explains your rights in relation to your personal information and how to contact us or the supervisory authority in the event you have a complaint.

2. About Scott+Scott UK LLP

- 2.1 The data controller in respect of personal information is Scott+Scott UK LLP, a limited liability partnership incorporated and registered in England and Wales under number OC402307. Our registered office is St. Bartholomew House 90-94, Fleet Street, London, England, EC4Y 1DH.
- 2.2 Scott+Scott UK LLP is:
 - (a) registered with the Information Commissioner’s Office (“**ICO**”) with registration number ZA149936;
 - (b) authorised and regulated by The Solicitors Regulation Authority with registration number 626637; and
 - (c) affiliated with the US law firm, Scott+Scott, Attorneys at Law, LLP (“**Scott+Scott US**”), whose principal place of business is in Connecticut.
- 2.3 References in this Policy to “**Scott+Scott**”, “**we**”, “**our**” and “**us**” are references to Scott+Scott UK LLP, the UK data controller.

3. Contacting us

- 3.1 Scott+Scott has appointed a Data Protection Officer whose contact details are set out below.
- 3.2 If you have any questions about this Policy or your information, or to exercise any of your rights as described in this Policy or under applicable data protection laws, you can contact us as follows:

Data Protection Officer
 Scott+Scott UK LLP, St. Bartholomew House, 90-94 Fleet Street, London, EC4Y 1DH
 By email: dpo@scott-scott.com
 By telephone: +1 646-582-0118

4. Data Protection Principles

- 4.1 Scott+Scott adheres to the following principles when processing your personal information:
 - (a) **Lawfulness, fairness and transparency** – information must be processed lawfully, fairly and in a transparent manner.
 - (b) **Purpose limitation** - information must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- (c) **Data minimisation** - information must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
 - (d) **Accuracy** - information must be accurate and, where necessary, kept up to date.
 - (e) **Storage limitation** - information must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information are processed.
 - (f) **Integrity and confidentiality** - information must be processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using appropriate technical or organisational measures.
- 4.2 This Policy describes the personal information that we collect, and explains how we comply with these principles.
- 5. Information we Collect**
- 5.1 We collect personal information as necessary to enable us to carry out your instructions, to manage and operate our business and to comply with our legal and regulatory obligations.
- 5.2 The personal information that we collect in the course of advising and/or acting for you includes, but is not limited to, the following:
- (a) full name;
 - (b) home and business address;
 - (c) contact details (such as telephone numbers and email address);
 - (d) date of birth;
 - (e) gender;
 - (f) marital status;
 - (g) copies of passport, national identity card, driving licence, utility bills, bank statements and similar documents;
 - (h) business and professional qualifications and experience;
 - (i) immigration status and work permits;
 - (j) information relating to the matter in which you are seeking our advice or representation including (where relevant) information relating to your case or dispute with another party;
 - (k) other personal information contained in correspondence and documents which you may provide to us depending on why you have instructed us; and
 - (l) information we obtain from our IT and communications monitoring.
- 5.3 This personal information is required to enable us to carry out your instructions. If you do not provide personal information we ask for, it may delay or prevent us from providing our services to you.
- 5.4 You confirm that you are authorised to provide to us the personal information which we shall process on your behalf.
- 5.5 Where the personal information relates to your directors, shareholders, beneficial owners, employees, agents, associates or family members it is not reasonably practicable for us to provide to them the information set out in this Policy. Accordingly, where appropriate, you are responsible for providing this information to any such person.

6. How your information is collected

- 6.1 We collect most of this information from you directly, however, we also collect information:
- (a) from publicly accessible sources (for example, Companies House);
 - (b) directly from a third party (for example, client due diligence providers);
 - (c) from a third party with your consent (for example, your bank or building society, another financial institution or advisor; or consultants and other professionals we may engage in relation to your matter);
 - (d) your employer, professional body or pension administrators;
 - (e) your doctors, medical and occupational health professionals;
 - (f) via our website - we use cookies on our website (for more information on cookies, please see our Website Privacy and Cookies Policy).
 - (g) via our information technology systems, for example:
 - (i) case management, document management and time recording systems;

7. Special categories of (“sensitive”) personal information

- 7.1 You may also supply us with, or we may receive, special categories of (or “sensitive”) personal information, which includes information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, health or sex life, sexual orientation, genetic data or biometric data.
- 7.2 We process these special categories of personal information on the basis of one or more of the following:
- (a) where you have given explicit consent to the processing of the personal information for one or more specified purposes;
 - (b) where the processing relates to personal information which is manifestly made public by you;
 - (c) where the processing is necessary for the establishment, exercise or defence of legal claims;
 - (d) where the processing is necessary for reasons of substantial public interest, in accordance with applicable law. Such reasons include where the processing is necessary:
 - (i) for the purposes of the prevention or detection of an unlawful act or for preventing fraud;
or
 - (ii) for the provision of confidential advice.

8. Information relating to criminal convictions & offences

- 8.1 We collect and store personal information relating to criminal convictions and offences (including the alleged commission of offences) only where necessary for the purposes of:
- (a) the prevention or detection of an unlawful act and is necessary for reasons of substantial public interest;
 - (b) providing or obtaining legal advice; or
 - (c) establishing, exercising or defending legal rights.

9. How and Why we use your information

- 9.1 Our use of your personal information is subject to your instructions, data protection laws and our professional duty of confidentiality.

9.2 We will only process your personal information if we have a legal basis for doing so, including where the processing is necessary for:

- (a) the performance of our contractual engagement with you: this relates to all personal information we reasonably need to process to carry out your instructions;
- (b) compliance with a legal obligation to which we are subject: this relates to our legal obligations in relation to, for example, anti-money laundering; and
- (c) the purposes of the legitimate interests pursued by us or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms: this relates to our processing for marketing purposes, for our management, accounting and administration purposes and for data security.

9.3 The table below further explains the purposes for which Scott+Scott will use your personal information (excluding sensitive personal information) and our legal basis for doing so:

Purposes for which we will process the information	Legal Basis for the processing
To provide legal professional services to you in connection with your matters.	For the performance of our contract with you or to take steps at your request before entering into a contract.
To carry out associated administration and accounting in connection with your matters and other processing necessary to comply with our professional, legal and regulatory obligations.	For the performance of our contract with you or to take steps at your request before entering into a contract. To comply with our legal and regulatory obligations.
To comply with our anti-money laundering requirements.	To comply with our legal and regulatory obligations.
To comply with our internal business policies.	It is in our legitimate interests or those of a third party to adhere to our own internal procedures so that we can deliver an efficient service to you. We consider this use to be necessary for our legitimate interests and proportionate.
For operational reasons, such as improving efficiency, training and quality control.	It is in our legitimate interests to be as efficient as we can so we deliver the best service for you. We consider this use to be necessary for our legitimate interests and proportionate.
To prevent unauthorised access and modifications to our systems.	It is in our legitimate interests to prevent and detect criminal activity that could be damaging for Scott+Scott and for you. We consider this use to be necessary for our legitimate interests and proportionate. To comply with our legal and regulatory obligations.

For updating client records.	For the performance of our contract with you or to take steps at your request before entering into a contract. To comply with our legal and regulatory obligations.
For marketing our services.	It is in our legitimate interests to market our services. We consider this use to be proportionate and will not be prejudicial or detrimental to you.
To carry out credit reference checks.	It is in our legitimate interests to carry out credit control and to ensure our clients are likely to be able to pay for our services.
External audits and quality checks, e.g. for accreditation and the audit of our accounts.	It is in our legitimate interests to maintain our accreditations so we can demonstrate we operate at the highest standards. To comply with our legal and regulatory obligations.

- 9.4 Where we request personal information to identify you for compliance with anti-money laundering regulations, we shall process such information only for the purposes of preventing money laundering or terrorist financing, or as otherwise set out in this Policy or permitted by law.
- 9.5 Where you provide consent, you can withdraw your consent at any time and free of charge, but without affecting the lawfulness of processing based on consent before its withdrawal. You can update your details or change your privacy preferences by contacting us as provided in section 3 above.
- 9.6 Scott+Scott acts as a data controller in relation to the processing of personal information as set in this Policy. However, in some circumstances we may process personal information on your behalf as a data processor for the purposes of data protection laws.

10. Marketing

- 10.1 We also use your personal information to notify you by email or post about important legal developments and services which we think might be of interest or value to you, including newsletters, invitations to seminars and similar marketing.
- 10.2 We have a legitimate interest in using your personal information for marketing purposes (please see section 9.3). This means we do not usually need your consent to send you marketing communications. However, where consent is needed, we will ask for this consent separately.
- 10.3 For marketing purposes, we may disclose personal information to Scott+Scott Attorneys LLP (our US office) or to third parties providing marketing services to us, or with whom we are conducting joint marketing exercises.
- 10.4 You have the right to opt out of receiving direct marketing communications from us at any time by:
- contacting the Data Protection Officer using the contact details set out in section 3 above; and
 - using the “unsubscribe” link in emails.

11. Email Monitoring

11.1 Emails which you send to us or which we send to you may be monitored by us to ensure compliance with professional standards and our internal compliance policies. Monitoring is not continuous or routine, but may be undertaken on the instruction of a partner where there are reasonable grounds for doing so.

12. Third Party Processors

12.1 Our information technology systems are operated by us but some data processing is carried out on our behalf by third parties. Details regarding these third party data processors can be obtained from our Privacy Officer whose details are given in section 3 above.

12.2 Where processing of personal information is carried out by a third party data processor on our behalf we endeavour to ensure that appropriate security measures are in place to prevent unauthorised access to or use of your data.

13. Disclosure of Personal Information

13.1 Personal information will be retained by us and will not be shared, transferred or otherwise disclosed to any third party, except as set out in this Policy.

13.2 If we are working with other professional advisers on your behalf we shall assume that we may disclose your information to them, unless you instruct us otherwise.

13.3 We may disclose and share personal information

- (a) with Scott+Scott partners, staff and consultants;
- (b) with partners, staff and consultants of Scott+Scott Attorneys at Law LLP and Scott+Scott Germany LLP. (see section 17 below re: transferring data out of EEA);
- (c) to other professional advisers and third parties (such as barristers, experts or insurance providers) in accordance with your instructions;
- (d) to our professional indemnity insurers, brokers or advisers, and auditors, lawyers or risk managers who we or they may appoint;
- (e) third party processors, service providers, representatives and agents that we use to make our business more efficient, e.g. e-disclosure or copying service providers, document collation or analysis suppliers; and
- (f) if we, acting in good faith, consider disclosure to be required by law or the rules of any applicable governmental, regulatory or professional body.

13.4 Should we be requested by certain authorities to provide them with access to your information in connection with the work we have done, or are doing, for you, we will comply with that request only to the extent that we are bound by law to do so and, in so far as it is allowed, we will notify you of that request or provision of information.

13.5 In certain circumstances, solicitors are required by statute to make a disclosure to the National Crime Agency where they know or suspect that a transaction may involve a crime including money laundering, drug trafficking or terrorist financing. If we make a disclosure in relation to your matter(s), we may not be able to tell you that a disclosure has been made.

13.6 We may also need to share some personal information with other parties, such as potential buyers of some or all of our business or during a re-structuring. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations.

13.7 We may transfer personal data to a successor firm or company which acquires the legal practice carried on by us. If this happens, we shall ensure that you are notified of the transfer and we shall

secure a commitment from the firm or company to which we transfer personal data to comply with applicable data protection laws.

14. Your Rights

14.1 Access to your information and updating your information:

- (a) You have the right to access information which we hold about you. If you so request, we shall provide you with a copy of your personal information which we are processing (this is commonly known as a “subject access request”);
- (b) You also have the right to receive your personal information in a structured and commonly used format so that it can be transferred to another data controller (this is called the right to “data portability”).
- (c) We endeavour to ensure that your personal information is accurate and up to date and you may ask us to correct or remove any information you think is inaccurate.

14.2 Right to object

- (a) You have the right to object at any time to our processing of your personal information used for direct marketing purposes (please see section 10 for further details).

14.3 Where we process your information based on our legitimate interests

- (a) You also have the right to object, on grounds relating to your particular situation, at any time, to processing of your personal information which is based on our legitimate interests. Where you object on this ground, we shall no longer process your personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

14.4 Your other rights

- (a) You also have the following rights under data protection laws to request that we rectify your personal information which is inaccurate or incomplete.
- (b) In certain circumstances, you have the right to:
- (c) request the erasure of your personal information (known as the “right to be forgotten”); and
- (d) restrict the processing of your personal information to which you have given us your consent or used for the establishment, exercise or defence of legal claims or used for the protection of the rights of others.

14.5 Please note that the above rights are not absolute, and we may be entitled to refuse requests, wholly or partly, where exceptions under applicable law apply.

15. Exercising Your Rights

15.1 You can exercise any of your rights as described in this Policy and under data protection laws by contacting the Data Protection Officer.

15.2 Except as described in this Policy or provided for under applicable data protection laws, there is no charge for the exercise of your legal rights. However, if your requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or taking the action requested; or (b) refuse to act on the request.

15.3 Where we have reasonable doubts concerning the identity of the person making the request, we may request additional information necessary to confirm their identity.

16. Security of your information

- 16.1 We store your information in hard copy and in electronic format. We use industry standard technical and organisational measures to protect information from the point of collection to the point of destruction.
- 16.2 We will only transfer personal information to a third party if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.
- 16.3 Unfortunately, the transmission of information via the internet is not completely secure. Although we will endeavour to protect your personal information, we cannot guarantee the security of your data transmitted over the internet.

17. Transferring your personal information outside of EEA

- 17.1 The information Scott+Scott UK LLP collects from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). Scott+Scott UK LLP (in the UK) routinely shares personal information of its clients and contacts with Scott+Scott Attorneys at Law LLP in the US and Scott+Scott Germany LLP in Germany and vice versa. Your information may also be transferred or accessed internationally in the context of a litigation matter which you are involved in or, for example, where our staff are accessing data whilst abroad.
- 17.2 Where personal information is transferred to and stored in a country not determined by the European Commission as providing adequate levels of protection for personal information (such as the USA), we take steps to provide appropriate safeguards to protect your personal information, including entering into standard contractual clauses approved by the European Commission. Scott+Scott UK LLP, Scott+Scott Germany LLP and Scott+Scott Attorneys at Law LLP are parties to a Data Transfer Agreement which incorporates the standard contractual clauses. To obtain a copy of those clauses, please contact our Data Protection Officer.
- 17.3 In addition, it is sometimes necessary for us to transfer and store your personal information outside the EEA as follows:
 - (a) with our service providers located outside the EEA;
 - (b) if you are based outside the EEA; or
 - (c) where there is an international aspect to the matter which we have been instructed on.
- 17.4 If you want further information on the specific mechanisms used by us when transferring your personal information out of the EEA, please contact our Data Protection Officer using the details set out in section 3 above.

18. Information Retention Periods

- 18.1 Personal information received by us will be retained for as long as necessary to fulfil our engagement. Following the end of our engagement we will retain information for six years. After the six year period the information will be destroyed unless there is a compelling reason for the firm to retain your information, for example:
 - (a) to enable us to respond to any queries, complaints or claims made by you or on your behalf; and
 - (b) if required for legal, regulatory, fraud and other financial crime prevention or other legitimate business purposes.
- 18.2 After this period, when it is no longer necessary to retain your personal information, we will securely delete or anonymise it.
- 18.3 Personal information processed for compliance with anti-money laundering and prevention of terrorist financing regulations will be destroyed five years after the end of the engagement unless:

- (a) we are required to retain the information by or under any enactment or for the purpose of any court proceedings;
- (b) the individual has given consent to the retention of the information, or
- (c) we have reasonable grounds for believing the information needs to be retained for the purpose of legal proceedings.

19. Complaints

- 19.1 If you have any questions or concerns regarding this Policy or our data protection practices, please contact us as provided in section 3 above. In addition, you have the right to complain to the Information Commissioner's Office (<https://ico.org.uk/>). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

20. Changes to this Policy

- 20.1 We may change this Policy from time to time. The current version will always be available from us in hard copy or on our website. We will post a prominent notice on the website to notify you of any significant changes to our privacy policy, or update you by other appropriate means.
- 20.2 This Policy was last updated on 23 April 2021.