Data Policy

2.14 The Data Protection Rights

2.14.1 The firm is a data controller in relation to the client information we process as well as staff details. See para 1.3.8 for the name of the person responsible for data protection within the firm. We are committed to maintaining the highest standards of data quality and information security. This policy, and its associated procedures and practices on the appropriate use of IT as set out in part 5 of this manual, are designed to protect the lawful and proper processing of client data, and that classified as personal date within the EU General Data Protection Regulation("GDPR") and the Data Protection Act 2018 ('DPA 2018') in particular.

2.14.4 The GDPR, which took effect in May 2018, places greater duties on businesses to abide by the data protection principles and ensure that all personal data is used fairly, lawfully and for the purposes notified to clients. The person responsible for data protection compliance within the firm is the Director. To ensure compliance with some of the key provisions a number of changes have been made to the firm's terms of business/retainer. The GDPR obligations are supplemented by the DPA 2018 and although EU inspired, the regime will remain in force notwithstanding Brexit.

2.14.5 We are also required by the GDPR to keep records of where and how the practice holds its personal data, as well as the lawful basis on which we hold data, in part as there is an obligation to be able to demonstrate that we comply with the obligations and also so that we can provide full and accurate responses to any data subject access requests from clients or others.

2.14.4 We comply with all relevant legislative and regulatory provisions governing the management and storage of data in both electronic and paper formats. We are registered with the Information Commissioner under the GDPR and the DPA 2018. We comply with the data protection principles, i.e. that all data covered by the GDPR (which includes not only computer data, but also personal data held in a filing system) is:

- Fairly and lawfully processed;
- Processed for stated purposes only;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject’s rights;
- Secure; and
- Not transferred to non-EU countries without adequate protection.

2.14.5 Paper files and other records or documents containing personal/sensitive data are kept securely and retained for as long as – but no longer than – necessary and the review process forms part of the quality compliance review process (see 1.7). Clients are informed of their data subject rights by way of privacy notices through our retainer letters and terms of business documents sent out at the outset of every matter. The privacy notice can also be found displayed on sharepoint and office.

2.14.6 There are rights for data subjects to make formal access requests for information on the personal data we hold upon them and we are obliged then to respond without undue delay and within the period of a month. In order to do so it is essential that any such request, even if not described as a "data subject access request" is passed to Director immediately upon receipt. We

will then respond to it by letter/email having first satisfied ourselves that the request is from the data subject concerned so as to avoid the risk of a serious data/confidentiality breach by sending to someone who is not entitled to it. No charge will be made for responding to any such request.

2.14.7 If a data breach occurs we may also need to treat it as a breach of the duty of confidentiality under outcome 4(1) of the Code of Conduct also and so amounting to a breach to be recorded by the COLP in that regard as well. Where the data breach is serious it may be necessary to report it to the ICO as required by Article 33, to the SRA as a material breach of our obligations under the Code of Conduct, to the firm's indemnity insurers and to the data subject in pursuance of Article 34 and outcome 1(16) of the Code of Conduct. Please therefore take the greatest care in relation to all communications to clients and others and see further the parts of the manual dealing with information security and IT use at sections 5.12-5.15 and report any known or suspected breach to the Director.

2.14.8 If planning major changes to the operation of the practice we will undertake a data protection impact assessment as required by Article 35 so that we incorporate data protection 'by design and default'.

2.14.9 The person in charge of data protection is the Director. Training will be conducted as required on the topics of data protection and information security. A number of short training videos on these and other compliance topics on the Infolegal website as part of our subscription to that service.

2.14.10 The Director(Johnpaul Ezeagu) is the Data Protection Officer of this firm. The data subjects including our clients have a number of rights, as follows:

- to be informed,
- of access,
- rectification,
- erase,
- restrict processing,
- data portability,
- to object, and
- certain rights in relation to automated decision making and profiling.

2.14.11 Right to be Informed (Articles 13-14)

The right to be informed is the right of the individual to require us to provide what is described as "fair processing information". This will be provided through our client care letter.

The information provided depends upon the nature of our engagement and whether the data was obtained directly or indirectly from the client and it includes:

- The identity and contact details of the data controller – and where relevant their representative and the firm's data protection officer;
- The purpose for which the data is obtained and the lawful basis for processing that data;
- Where relevant, the legitimate interests of the controller;
- Details of anyone with whom the data will be shared;
- Details of any other countries to which the data will be sent and the safeguards to protect that data;
- The period for which the data will be retained;
- Where relevant, the right for the data subject to withdraw consent;
- The right to lodge a complaint;
- If not from the data subject themselves, where the data originated from; and
- Whether any of the data will be used in an automated decision-making process.

This information must be provided either at the time at which the data is obtained in the case of directly obtained information or within 14 days after it is obtained if obtained from elsewhere. In addition, if the information is used to communicate with the data subject or it is to be disclosed to a third party, then if not already provided the information should be given then.

2.14.12 Right of Access (Article 15)

The data subjects including clients have rights to obtain from the controller confirmation as to whether or not their personal data is being processed, and if so their right to access that data and receive information relating to the purpose for the processing, the categories of data, the identity of anyone with whom the data has been shared, the period for which it will be stored, the right to rectification or erasure of that data, the right to complain, where the data came from (if not from the data subject) and whether or not the data is to be used in any form of automated decision-making process.

In the event that we receive a request for this information then we must deal with that request within one month and we must not charge for the supply of that information unless the request is manifestly unfounded or excessive, in which case we may make a reasonable charge.

2.14.12 Right to Rectification (Article 16)

This is simply the right for a data subject including clients to request that inaccuracies, or a lack of completeness, in the data we hold to be remedied. We must inform any third parties to whom we have supplied the data of the facts of the rectification and inform the data subject that we have done so. We have one month in which to carry out the rectification, unless it is complex, in which case we have up to two months. In the event that we will not be carrying

out the rectification we must inform the data subject of the reasons for this and their right to complain or apply for a judicial remedy.

2.14.12 Right to Erasure

Also known as the right to be forgotten, this is the right of data subjects including clients to request erasure of personal data in certain circumstances including where:

- the data is no longer needed for the purpose for which it was obtained;
- the data subject withdraws consent, if consent is the basis for the data being held;
- the data subject objects to the processing and there is no overriding legitimate reason for continuing to process the data;
- the data was obtained in breach of the GDPR;
- it must be erased to comply with a legal obligation; and
- it relates to "information society services" to a child

There are also a number of circumstances where we can refuse a request to erase. These include:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for public health purposes in the public interest;
- certain archiving purposes; and
- the exercise of defence of legal claims.

We must also give consideration as to whether complying with a request for erasure could prejudice the rights of another person – for example where a matter relates to two people and only one wants the common data to be erased.

2.14.13 Right to Restrict Processing (Article 18)

Falling short of erasure, this gives the data subjects including clients the right to block or suppress the processing of their data. In these circumstances you would be entitled to retain the data but not do anything with it. This may arise where, for example, the accuracy of the data is in dispute, where there is an objection to the processing, where the processing is unlawful but the data subject does not want erasure or where you no longer require the data but the data subject requires you to retain it for the purposes of a legal claim.

As with deletion, we must advise third parties of the restriction unless to do so is impossible or involves a disproportionately large amount of effort.

2.14.14 Right to Data Portability (Article 20)

This is the right of data subjects including clients to obtain and reuse their data for their own purposes across different services. It applies where the data has been supplied by the individual with their consent or for the performance of a contract and the processing is carried out by automated means.

2.14.14 Right to Object (Article 21)

Data subjects including client have the right to object to data being processed:

- based on legitimate interests or the performance of tasks in the public interest/exercise,
- in relation to direct marketing, and
- in relation research and statistics.

If such an objection is raised by a client then we must stop processing the data unless we can show compelling legitimate grounds that override the individuals interests, rights and freedoms, or the processing is for the establishment, exercise or defence of a legal claim.

The right to object is something that must be brought to the attention of the data subject at the point of first contact and in our client care letter "clearly and separately from any other information".

2.14.15 Automated Decision Making (Article 22)

This is of limited applicability to the work of most law firms but is the subject of ICO guidance if required.

Appendix A1 - Data Collection Form

Data Controller Name[1]:	**Johnpaul Ezeagu**	**Department[2]:**	**Civil/Criminal Law**

Type of Information	**Information**
Purpose of Processing[3]	
Category of Individual[4]	
Category of Personal Data[5]	
Access to Data[6]	
Where Data Sent[7]	
Contract with External Processor[8]	

Data Policy

Source of the Personal Data[9]
Location of Personal Data[10]
Nature of Data Storage[11]
Data Security[12]

Notes to Data Form

1. **Data Controller Name** - Please supply name of the person who is primarily responsible for the data - probably you in most cases but perhaps your cashier or officer supervisor as well.

2. **Department or function** - Fee earning for the most part but perhaps also HR, accounts or marketing

3. **Purpose of Processing** - Please give the reason why the data is being processed. Reasons for processing data could include the following (the list is not exhaustive):

    - Client Work: acting for client, carrying out conflict of interest check, providing costs estimate, general client administration, AML checks, due diligence, AML report to NCA, acting as an agent for a data controller, instructing a third party such as expert witness or counsel

    - Accounts: Billing client or former client, accounting to beneficiaries under an estate, paying a third-party bill, pursuing unpaid costs, dealing with an undertaking to pay money

    - HR: payroll, personnel file, recruitment, reference, tax, pension

    - Marketing: sending out newsletter, informing of services, direct marketing

    - Administration: employing contractor, contacting computer engineer, contact at burglar alarm company

4. **Category of Individual** - Please specify the type of individual whose personal data is being processed. For example Client, Employee, Interview Candidate, , Barrister, Expert Witness, Potential Client, Newsletter Recipient etc.

5. **Category of Personal Data** - Please indicate the type of personal data that is being processed. This could include Contact Details, Nature of Matter, Criminal Record, Salary Details, Tax Information, Qualifications, Employment History, Ethnicity etc.

6. **Access to Data** - Please indicate everyone who has access to the personal data. Give their role rather than their name. For example, principal, fee-earner, cashier, administrator, secretary, receptionist.

7. **Where Data Sent** - If the information is going to be shared with a third party, please indicate the nature of that third party. For example, solicitor for other party, other legal adviser, National Crime Agency, HMRC, Provider of Employment Reference, Marketing Company

8. **Contract with External Processor** - if the information is going to be processed by a third party please indicate the nature of the processing - e.g. outsourced due diligence, representation as agent at local court, process serving - and confirm that a contract exists which contains the specific minimum terms as required by the GDPR. See Appendix G for more information on relationships with processors.

9. **Source of the Personal Data** - if relevant, you should specify where the personal data has originated. For example, Data Subject, Third Party (in which case specify nature of third party), Another Data Controller (in which case specify reason for its provision - such as agency instruction), Recruitment Consultant

10. **Location of Personal Data** - you need to specify where the data is held - for example accounting system, emails, filing system, HR Records, matter processing system

11. **Nature of Data Storage** - please specify how the data is stored - for example manual records, in a folder, electronic records (specifying system), hard-drive, memory stick, personal device, laptop, cloud hosting, etc

12. **Data Security** - please specify what, if any, data security applies to the storage of the information - for example encryption, behind a firewall, passworded memory stick etc

Additional considerations

In addition, you will need to consider the following when you have collected or have received the responses:

13. **Retention Period/Method of Calculation** - Article 5(1)(e) of the GDPR requires that data which permits the identification of data subjects should be retained for no longer than is necessary for the purposes for which the personal data is processed. Please specify the period for which this data is to be retained (or the period calculated if not known at this time) e.g. 6 years, 7 years after completion of matter, etc).

14. **Deletion/Retention Policies** - Consider whether you have a data deletion/retention policy which will apply to the data in question.

15. **Methods/Responsibilities for Updating** - Please indicate how the data is kept up to date and who will do so and how.

16. **Lawful Basis for Processing** - It is a core provision of the GDPR that you have a lawful basis for processing personal data. Please specify here which of the 6 lawful bases the firm is relying upon in relation to this data. Those bases are:

    - consent - the data subject has given clear consent for their personal data to be processed (for example someone who has given clear consent to being sent marketing materials)
    - contract - the processing is necessary in connection with a contract you have with the data subject (can include clients as well as staff and third parties)
    - legal obligation - where the processing is necessary for you to comply with the law (for example sending details of pay to HMRC or a MLR disclosure to the NCA)
    - vital interests (processing the data subjects' information to protect their life
    - public task - where the processing is necessary to perform a task in the public interest
    - legitimate interests - the processing is necessary for your or a third party's legitimate interests unless overridden by a good reason for protecting the individual's personal data

17. **If Basis Consent, date of Consent** - If the firm is relying upon consent, the date of that consent needs to be recorded. It would be useful, if there is a database of consents, for there to be some link to the relevant consent. This will relevant to any marketing lists you operate.

18. **Basis for Processing Special Character Data** - The GDPR provides that unless one of the specific exemptions applies, the processing of

personal data revealing 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 natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited. If, therefore, the data held refers to any of these prohibited forms of data then the basis for processing must be given. These include:

- explicit consent,
- necessity for the purposes of carrying out employment/social security/social protection obligations,
- protection of vital interests,
- personal data made public by the data subject

19. **Legitimate Interest for the Processing** - If the firm is relying upon legitimate interest for processing the data subject's personal data then it must identify what that legitimate interest is, that the processing is necessary to achieve it and that it has been balanced against the data subject's interests, rights and freedoms. A legitimate interest's assessment may need to be undertaken to demonstrate this.

20. **Has Data Breach Occurred?** - Has the data ever been the subject of any form of a data breach - for example hacking, loss of file, loss of device containing the data. if so, please supply details including whether ICO/data subject informed, damage caused, method by which data was recovered, etc.

21. **Processed in non-EU Country and Safeguards Put in Place** - if any of the personal data is to be transferred outside of the EU to those operating in non-EU countries or to international organisations, which country is it being transferred to, what is the purpose for the transfer and have adequate safeguards been put in place?