GDPR & Data Protection Policy

Pittalis LLP

Issue Date	31/01/2022
Approved By	Roger Pittalis
Managed By	The Strategic Partner
Next Review Date	30/11/2022
Version Control	Version 3

1. Introduction

This Policy sets out the obligations of **Pittalis LLP** a law firm whose head office is at Global House, 303 Ballards Lane, London, N12 8NP, ("the Firm") regarding data protection and the rights of clients ("data subjects") in respect of their personal data under UK General Data Protection Regulation (GDPR) which sits alongside The Data Protection Act 2018 (DPA 2018).

The UK GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Firm's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Firm, its employees, agents, contractors, or other parties working on behalf of the Firm.

The Firm is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the UK GDPR. The UK GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. The Rights of Data Subjects

The UK GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

- The right to be informed (Part 12).

- The right of access (Part 13);
- The right to rectification (Part 14);
- The right to erasure (also known as the 'right to be forgotten') (Part 15);
- The right to restrict processing (Part 16);
- The right to data portability (Part 17);
- The right to object (Part 18); and
- Rights with respect to automated decision-making and profiling (Parts 19 and 20).

4. Lawful, Fair, and Transparent Data Processing

The UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes;
- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law;
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of

the data subjects;

- The processing relates to personal data which is clearly made public by the data subject;
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for substantial public interest reasons, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;
- The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5. Specified, Explicit, and Legitimate Purposes

The Firm collects and processes the personal data set out in Part 19 of this Policy. This includes:

- Personal data collected directly from data subjects; and
- Personal data obtained from third parties.

The Firm only collects, processes, and holds personal data for the specific purposes set out in Part 19 of this Policy (or for other purposes expressly permitted by the UK GDPR).

Data subjects are kept informed at all times of the purpose or purposes for which the Firm uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

The Firm will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 19, below.

7. Accuracy of Data and Keeping Data Up-to-Date

The Firm shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

The Firm shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of the Firm's approach to data retention, including retention periods for specific personal data types held by the Firm, please refer to our Data Retention Policy.

9. Secure Processing

The Firm shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 21 to 25 of this Policy.

10. Accountability and Record-Keeping

The Firm's Data Compliance Manager is **Roger Pittalis** (roger@pittalis.co.uk)

The Data Compliance Manager shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Firm's other data protection-related policies, and with the UK GDPR and other applicable data protection legislation.

The Firm shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Firm, its Data Compliance Manger, and any applicable third-party data processors;
- The purposes for which the Firm collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the Firm, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Firm (please refer to the Firm's Data Retention Policy); and
- Detailed descriptions of all technical and organisational measures taken by the Firm to ensure the security of personal data.

11. Data Protection Impact Assessments (DPIA)

The Firm shall carry out **Data Protection Impact Assessments** for any and all new projects and/or new uses of personal data where the implementation will result in a significant change in the way the Firm processes data and/or where there is a high risk to data protection and control.

Data Protection Impact Assessments shall be triggered and overseen by the Data Compliance Manager and shall address the following:

- The type(s) of personal data that will be collected, held, and processed;
- The purpose(s) for which personal data is to be used;
- The Firm's objectives;

- How personal data is to be used;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to the Firm; and
- Proposed measures to minimise and handle identified risks.

When performing the DPIA, the Firm will use the DPIA template (see **Appendix 3**) to direct the assessment and cover all key areas.

12. Keeping Data Subjects Informed

The Firm shall provide the information set out to every data subject:

- Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
    - if the personal data is used to communicate with the data subject, when the first communication is made; or
    - if the personal data is to be transferred to another party, before that transfer is made; or
    - as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided:

- Details of the Firm including, but not limited to, the identity of its Data Compliance Manager;
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 19 of this Policy) and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which the Firm is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;
- Where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see Part 26 of this Policy for further details);
- Details of data retention;
- Details of the data subject's rights under the UK GDPR;
- Details of the data subject's right to withdraw their consent to the Firm's processing of their personal data at any time;

- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the UK GDPR);
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access Requests

Data subjects may make **Subject Access Requests** (SARs) at any time to find out more about the personal data which the Firm holds about them, what it is doing with that personal data, and why.

Data subjects wishing to make a SAR may do so in writing, using the Firm's **Subject Access Request Form** (see ***Appendix 1***), or other written communication. SARs should be addressed to the Firm's Data Compliance Manager by email roger@pittalis.co.uk.

Responses to SARs shall normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

All SARs received shall be handled by the Firm's Data Compliance Manager.

The Firm does not charge a fee for the handling of normal SARs. The Firm reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

Data subjects have the right to require the Firm to rectify any of their personal data that is inaccurate or incomplete.

The Firm shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Firm of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

Data subjects have the right to request that the Firm erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for the Firm to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to the Firm holding and processing their personal data;
- The data subject objects to the Firm holding and processing their personal data (and there is no overriding legitimate interest to allow the Firm to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);

- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for the Firm to comply with a particular legal obligation.

Unless the Firm has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

Data subjects may request that the Firm ceases processing the personal data it holds about them. If a data subject makes such a request, the Firm shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

The data subject shall have the right to receive personal data concerning them, which they provided to the Firm, in a structured, commonly used and machine-readable format and have the right to transmit such data to another controller without hindrance from the Firm.

This right only applies to data which is held electronically and that the data subject has provided directly to the Firm.

For the purpose of accessing data held by the Firm for data portability purposes, the data subject is entitled to data which has been provided to the Firm: -

- actively and knowingly by the data subject.
- observed data whereby the data subject indirectly provides data when using a service or device which provides personal data on the data subject.

In exercising the data subject's right to data portability, the data subject shall have the right to have the personal data transmitted directly, where technically feasible, from the Firm; -

- to another data controller into their system or database.
- to the data subject directly into their system or database.

Exercising the right to data portability does not automatically lead to the erasure of the concerned data and that the Firm may still hold the data pursuant to Part 19.

A data portability request should be formally requested to the Firm's Data Compliance Manager by roger@pittalis.co.uk.

Any request which is considered manifestly unfounded or excessive can be declined or a reasonable fee charged to deal with the request.

This right shall not adversely affect the rights and freedoms of others.

18. Objections to Personal Data Processing

Data subjects have the right to object to the Firm processing their personal data based on legitimate interests, direct marketing (including profiling), [and processing for scientific and/or historical research and statistics purposes].

Where a data subject objects to the Firm processing their personal data based on its legitimate interests, the Firm shall cease such processing immediately, unless it can be demonstrated that the Firm's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to the Firm processing their personal data for direct marketing purposes, the Firm shall cease such processing immediately.

19. Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Firm (for details of data retention, please refer to the Firm's Data Retention Policy):

Data Ref.	Type of Data	Purpose of Data
001	Names and addresses	To communicate with clients and other parties
002	Telephone Numbers	To communicate with individuals
003	Usernames	To access an individuals or companies accounts such as social media
004	Passwords	To access an individuals or companies accounts such as social media
005	Email addresses	To communicate with individuals

20. Data Security - Transferring Personal Data and Communications

The Firm shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing personal data must be;
- All emails containing personal data must be marked "confidential";
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient and
- All personal data to be transferred physically, whether in hardcopy form or on removable

electronic media shall be transferred in a suitable container marked “confidential”.

21. Data Security - Storage

The Firm shall ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords and data encryption;
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- All personal data stored electronically should be backed up daily with backups stored offsite. All backups should be encrypted;
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Firm or otherwise and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Firm where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the UK GDPR (which may include demonstrating to the Firm that all suitable technical and organisational measures have been taken).

22. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Firm’s Data Retention Policy.

23. Data Security - Use of Personal Data

The Firm shall ensure that the following measures are taken with respect to the use of personal data:

- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Firm requires access to any personal data that they do not already have access to, such access should be formally requested to the Firm’s Data Compliance Manager by email – roger@pittalis.co.uk.
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Firm or not, without the authorisation of the Firm’s Data Compliance Manager by email – roger@pittalis.co.uk.
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer screen before leaving it; and
- Where personal data held by the Firm is used for marketing purposes, it shall be the

responsibility of the person providing the information to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

24. Data Security - IT Security

The Firm shall ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Firm, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Firm's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
- No software may be installed on any Firm-owned computer or device without the prior approval of **Roger Pittalis**.

25. Organisational Measures

The Firm shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of the Firm shall be made fully aware of both their individual responsibilities and the Firm's responsibilities under the UK GDPR and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, agents, sub-contractors, or other parties working on behalf of the Firm that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Firm;
- All employees, agents, contractors, or other parties working on behalf of the Firm handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of the Firm handling personal data will be appropriately supervised;
- All employees, agents, contractors, or other parties working on behalf of the Firm handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- All personal data held by the Firm shall be reviewed periodically, as set out in the Firm's Data Retention Policy;
- The performance of those employees, agents, contractors, or other parties working on behalf of the Firm handling personal data shall be regularly evaluated and reviewed;

- All employees, agents, contractors, or other parties working on behalf of the Firm handling personal data will be bound to do so in accordance with the principles of the UK GDPR and this Policy by contract;
- All agents, contractors, or other parties working on behalf of the Firm handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Firm arising out of this Policy and the UK GDPR; and
- Where any agent, contractor or other party working on behalf of the Firm handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Firm against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

26. Transferring Personal Data to a Country Outside the UK

The Firm may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the UK.

The transfer of personal data to a country outside of the UK shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the UK has determined ensures an adequate level of protection for personal data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the UK; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the UK GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- The transfer is made with the informed consent of the relevant data subject(s);
- The transfer is necessary for the performance of a contract between the data subject and the Firm (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- The transfer is made from a register that, under UK law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

27. Use of Personal Email or Personal Storage Devices

Under no circumstances is a member of staff permitted or authorised to send or CC any email relating to a client or a matter to a personal email address or copy/save any client or matter document to a personal storage device including cloud accounts.

Saving or sending information or document in such a manner is a breach of this policy and the firms confidentiality and privacy policy.

28. Data Breach Notification

All personal data breaches must be reported immediately to the Firm's **Data Compliance Manager,** using the **Data Breach Notification Form – see *Appendix 2***.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Compliance Manager must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Firm's Data Compliance Manager (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by the Firm to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

29. Reporting to the Information Commissioner's Office (ICO) & Solicitors Regulation Authority (SRA)

It is the responsibility of the **Data Compliance Manager** (usually in conjunction with the **Compliance Officer for Legal Practice [COLP])** to make a decision on whether a sate breach is reportable to the ICO. To decide on whether a report to the ICO is necessary, which must usually occur within 72 hours of the breach being discovered, the **Data Compliance Manager** will need to consider the following questions: -

- Has there been a personal data breach? - A personal data breach (PDB) can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.
- Does the breach involve the personal data of living individuals?
- Following the assessment, is there likely to be a high risk to individuals' rights and freedoms?

The answers to these questions will dictate whether a report to the ICO is necessary.

With regards to making reports to the SRA, this will be decided by the COLP and will apply to a data breach that is regarded as 'serious' which will ordinarily be dictated by the scale of the incident, how much data is affected, the number of people affected and the potential damage caused as a result of

the breach, financial or otherwise.

30. Version Control & Updates

This policy is reviewed annually and updated as necessary.

In the event of any statute or regulation changes, this policy will be brought up to date at that point in time and all the policies affected will also be updated.

A printed version of this policy should be considered obsolete.

Appendix 1: Data Subject Access Request Form

Data Subject Access Request Form

Please complete this form if you wish to request access to your personal data. You do not have to use this form, but it will help us to deal with your request as quickly and effectively as possible if you do.

You can also use this form if you are requesting access to personal data on behalf of someone else. In that case, we will need you to confirm you have that person's authority to ask for access to their data.

If you have any questions about this form or your request, please contact our **Data Compliance Manager, Roger Pittalis**, to discuss it further.

1 About You

Please provide the following information. If you have an account number or other reference number, please provide it.

Full name	[*Details to be inserted here*]
Address	[*Details to be inserted here*]
Contact details	[*Details to be inserted here*]
[[Customer account number OR Client number OR National Insurance number OR [*insert details of other relevant reference number, if any*]**]**	[*Details to be inserted here*]

For security reasons, we cannot respond to a request unless we have confirmed your identity. Please provide:

- certified copy driving licence or passport
- a utility bill or other proof of address (e.g., bank statement) dated within the last 3 months

2 Whose Personal Data Are You Requesting?

Please provide the following information. If you are making this request on behalf of someone else, we will need this information before we can supply you with the data you are asking for.

Are you requesting access to your own personal data?	☐ Yes, please go to section 3 below. ☐ No, please complete the rest of this section of the form.

If you are not requesting access to your own personal data, please provide the following information about the person on whose behalf you are making this request:

Full name	[*Details to be inserted here*]
Address	[*Details to be inserted here*]
Contact details	[*Details to be inserted here*]
[Customer account number OR Client number OR National Insurance number OR [*insert details of other relevant reference number, if any*]**]]**	[*Details to be inserted here*]
Age (if under 16)	[*Details to be inserted here*]

We cannot respond to your request until we also receive satisfactory confirmation of the identity of the person on whose behalf you are making this request. Please provide:

- a certified copy of their driving licence or passport
- a utility bill or other proof of their address**,** e.g., bank statement

Please provide a copy of your legal authority to make this request. This might be a signed letter of authority from the person on whose behalf you are making this request, a power of attorney, or confirmation that you are their legal representative.

3 What Data Are You Requesting?

Your rights to request access to personal data and other information are set out [*insert details, e.g., in our Privacy policy, available on our website*]. Please describe what personal data and other information you are requesting, in particular if you are asking for specific documents or information.

Description of the personal data and information requested including details of any specific documents or information you are asking for (where relevant)	[*Details to be inserted here*]

Please give as much detail as possible about where the data might be located and any other relevant information. You do not have to provide this information but doing so will help us to deal with your request as quickly and effectively as possible.

Location of data, e.g., any particular departments or parts of the organisation you have dealt with (if known)	[*Details to be inserted here*]
Relevant time periods, eg when we are likely to have obtained your data (if known)	[*Details to be inserted here*]
Dates of any particular correspondence, meetings or telephone calls (if known)	[*Details to be inserted here*]
The name(s) of people you have dealt with within our organisation (if known)	[*Details to be inserted here*]
Any other relevant information you can think of that might help us respond to your request	[*Details to be inserted here*]

4 Signature

Please check the information you have provided and sign below.

Signed	[*Signature to be inserted here*]
Date	[*Date to be inserted here*]

Please send this form and the documents we have asked you to provide to: [*insert contact details including postal and email address*].

If you are making this request by email, we will provide the information to you in an electronic format unless you ask us not to. If you wish to receive your information in a different format, e.g., hard copy please let us know in the box below.

[*Details to be inserted here*]

Appendix 2: Data Breach Notification Form

Data Breach or Potential Data Breach Notification Form

Please email this form to pittalis@thestrategicpartner.co.uk					
Guidance Required	Yes	No	**Information Only**	Yes	No

Notification

Notifier's Name		**Date of notification**	
Client: **(If applicable)**			
Matter number **(If applicable)**			
Reason for making notification			
Please attach any documentation relevant to the matter if not sending the whole file			
Date		**Signed**	

Outcome

Data Compliance Manager		**Date Received**	
Investigation notes and outcome			

Date recorded on the register		**Number of clients affected**	
Notification to Client(s) required	**Yes / No**	**Further Action required**	**Yes / No**
Notification required to COLP	**Yes / No**	**Report to ICO necessary**	**Yes / No**
Details of Action taken			
Signed		**Date Closed**	

Appendix 3: DPIA Template

Data Protection Impact Assessment

Name of Data Protection Officer/Data Compliance Manager	
Date Assessment Commenced	
Date Assessment Concluded	

Please answer each of the following questions to complete the DPIA.

In the event of a High Risk concern and/or changes to the way in which the Firm will process data, this will need to be discussed with appropriate stakeholder.

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. **Summarise why you identified the need for a DPIA.**

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it is not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you provide to individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
Data Compliance Manager/Data Protection Officer advice provided:		Data Compliance Manager/Data Protection Officer should advise on compliance, measures and whether processing can proceed
Summary of Data Compliance Manager/Data Protection Officer's advice:		
Data Compliance Manager/Data Protection Officer's advice accepted or overruled by:	Yes/No	**If overruled, you must explain your reasons below.**
Comments:		
Consultation responses reviewed by:		**If your decision departs from individuals' views, you must explain your reasons below.**
Comments:		
This DPIA will kept under review by:		**The Data Compliance Manager/Data Protection Officer should also review ongoing compliance with DPIA**