**PROTECTION & INVESTMENT LTD**

**GENERAL DATA PROTECTION REGULATION (GDPR) POLICY**

## 1. Introduction

The General Data Protection Regulation (GDPR) represented a wholesale change to the data protection framework that had been in place since 1998. It touches upon the storage and handling of personal data, extends the scope of data protection law within the UK and introduced more draconian penalties for those who fail to comply with it.

The PIL Board is ultimately responsible for ensuring that the firm complies with the requirements of the GDPR that came into force on 25th May 2018.

This policy document constitutes PIL's response to the requirements set down in the GDPR when applied to our business and the industry we are in. It focuses on two distinct Data Subject groups; **'members'** of PIL and PIL **'clients'**. The rights and treatment of each group are distinguished from the other where appropriate. They are commonly referred to as 'Individuals' or 'Data Subjects'.

## 2. What is Personal Data?

The GDPR is concerned with the protection of 'Personal Data', defined as:

*Data which relates to a living individual who can be identified*

*(a) from that data, or*

*(b) from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.*

## 3. Who does the GDPR apply to?

3.1 The GDPR applies to data processing carried out by organisations within the UK. It also applies to organisations outside the UK that offer goods or services to individuals within the UK. It started out as an EU Directive which passed into UK law in 2018. Following the UK's departure from the EU in January 2020 it is now commonly referred to as GDPR (UK) distinguishing it from the GDPR applicable in the EU.

3.2 Organisations are deemed to be either 'Data Controllers or 'Data Processors'

3.3 A Data Controller determines the purposes and means of processing Personal Data.

3.4 A Data Processor is responsible for processing personal data on behalf of a Controller.

3.5 PIL is a Data Controller as are the various Providers and Lenders the firm places business with.

3.6 Data processors are invariably those firms we contract to provide us with a service in the course of providing our clients with advice and a service. Examples include Intelligent Office, Volume, SmartSearch, Genovo, FE Analytics, Selectapension, Trigold, and Assureweb.

3.7 The GDPR places specific legal obligations on Data Processors, for example, they are required to maintain records of personal data and processing activities. They will have a legal liability in the event of a breach.

3.8 As a Data Controller we are not relieved of our obligations where a processor is involved. The GDPR places further obligations on us to ensure that our contracts with processors comply with the GDPR.

A due diligence exercise has been carried out to ensure that PIL's Data Processors are compliant with the obligations and requirements laid down in Article 28 of the GDPR (details further down). This is an ongoing exercise as our data processors change over time.

## 4. What is meant by 'processing' data?

The GDPR makes repeated use of the term 'processing' data. This covers a wide range of operation performed on personal data by manual or automated means. These are as follows:

- Collection and recording
- Organisation and structuring
- Storage
- Use
- Disclosure
- Alteration & Erasure

## 5. Data Subjects

5.1 A Data Subject is a living individual to whom personal data relates. PIL processes the Personal Data of two distinct groups, clients and members.

5.2 Personal Data belonging to Clients is processed in order to be able to provide them with its advisory and ongoing services. This a legal & regulatory requirement.

5.3 Personal Data belonging to members of PIL is processed as a pre-condition of joining PIL. As a business we required to know who we are employing; their name, bank details, if they are eligible to work in the UK and if they are a Fit & Proper person to working for a regulated firm which processes Personal Data on a day-to-day basis.

## 6. Types of Data

6.1 Personal data can include: **(This list is not exhaustive)**

- Personal details, e.g. name, address, date of birth, NINO
- Family and lifestyle including special categories of personal data
- Education and training
- Employment details, history & records
- Financial details and status
- Needs, objectives and aspirations

6.2 Certain categories of data are deemed more **sensitive** and there are much stricter rules in place as to when this data can be processed. These "special categories" consist of personal data that reveals:

- Racial or ethnic origin
- Political opinions
- Religious and philosophical beliefs
- Trade union membership
- Genetic data (inherited or acquired genetic characteristics)
- Biometric data (fingerprints & retina) for the purpose of uniquely identifying a natural person
- Sex life and sexual orientation
- Health and medical details

In addition, there is a further category relating to criminal convictions

**Typically, the only sensitive data we process for clients are their religious beliefs, sex life and sexual orientation and health and medical details. This must not be processed until it becomes absolutely necessary and only after Explicit Consent has been given by the client. If the data is not required it must not be processed.**

Members of PIL are required to undergo Criminal Record checks when they join. Senior Managers and Certified individuals are required to undergo this on a bi-annual basis thereafter. This is a regulatory requirement in order to establish if the applicant/adviser is and continues to be Fit & Proper to be part of and advise on behalf of a regulated firm. **Explicit Consent will be required to conduct these checks.**

Member of PIL may also have their Sensitive data processed where this data is required for underwriting purposes. **Where this applies Explicit Consent will be required.**

## 7. Principles of the GDPR

The data protection principles set out our main responsibilities. These state that personal data shall be:

- Processed lawfully, fairly and in a transparent manner.

- Collected for specified, explicit and legitimate purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up to date.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- 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.

The GDPR introduced an accountability principle; it requires us to demonstrate that we comply with the above principles, this is expanded on in the sections below.

## 8. Data Protection Officer (DPO)

8.1 PIL has not nominated a DPO as there is no obligation for us to do so. This would only be required if:

- we were a public authority (except for courts acting in their judicial capacity);
- our core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- our core activities consist of **large-scale** processing of special categories of data or data relating to criminal convictions and offences.

8.2 Processing of special categories of data (Sensitive Data) only occurs where the proposed financial contract being recommended requires it. An example would include Long Term Care Annuities and Life Assurance. These types of contracts represent only a small percentage of our overall business activity, impacting on a small percentage of our clients and for this reason we do not require a Data Protection Officer.

## 9. Lawful grounds claimed by PIL

In order to legally process Personal Data, we are required to have lawful grounds. There are a number of lawful grounds that can be cited, only 1 is required and those of most relevance to PIL are as follows:

9.1 Consent

Consent must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions and the ability to withdraw consent must be made simple.

**PIL does not require consent from past and present clients or from its members as there are other lawful grounds we can cite.** That said, it can be argued that we have client consent

through clients signing Client Agreements. The Client Agreement confirms the clients right to terminate the contract at any time.

9.2 Performance of Contract

The ability to process personal data is necessary to perform the contract between PIL and our clients. The Client Agreement is the contract and for that reason, as well as it being a regulatory requirement, it must always be provided to clients at the earliest stage and a signed copy received in return.

A further scenario exists; if an individual requests information from an adviser (prior to entering a contract/receiving and signing a Client Agreement) about a particular product, the processing of that individual's personal data is permitted for the purposes of responding to that **enquiry.**

**Performance of Contract is PIL's first justification for processing personal data belonging to clients. It might also be cited as lawful grounds for certain types and uses of data belonging to members of PIL or those looking to join.**

9.3 **Compliance with Legal & Regulatory Obligations**

It is a regulatory requirement that in order to provide clients with suitable advice we need to collect personal and financial information from clients. Aside from the 'Know Your Client' rule we have also required to collect data enabling us to satisfy Anti-Money Laundering Regulations. The same applies to the collection of data required under any other regulation which we are legally required to comply with. **Compliance with Legal & Regulatory Obligations is PIL's second justification for processing personal data belonging to clients.**

**Compliance with Legal & Regulatory Obligations is also a basis for processing certain types of personal data for members of PIL.** Specifically, this relates to compliance with the Fit & Proper rules for advisers and to a lesser extent administrative staff. As a regulated firm we are required to take steps to verify our member's financial status and that they do not have a record of criminal convictions.

9.4 Legitimate Interests

Legitimate interests are the most flexible lawful basis for processing, but it cannot be assumed it will always be the most appropriate. There are three elements to the legitimate interests' basis. We need to:

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

Legitimate interests can be our own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.

The processing must be necessary. If we can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

We must balance our interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.

Legitimate interests are likely to be most appropriate where we use an individual's data in a way they would reasonably expect and which has a minimal privacy impact, or where there is a compelling justification for the processing.

The following data processing activity will be done under Legitimate Interests:

- Direct Marketing – issue of Newsletters
- Recruitment – processing data of PIL applicants
- Retention of data – keep client and PIL member data indefinitely to help us defend a potential claim in the future
- Contact those who took out a mortgage with us and whose term is close to expiry.

We are required to keep a record of our legitimate interests' assessments (LIA) and include details of our legitimate interests in our privacy notice. These are located in the appendix.

**Special categories of personal (Sensitive) data**

Where special categories of personal data or data relating to criminal convictions are processed, it may be under one of the following conditions:

9.5 Explicit Consent

Explicit consent requires a very clear and specific statement of consent. It must be expressly confirmed in words, rather than by any other positive action which is all that is required for 'Consent'.

There is no set time limit for consent. How long it lasts will depend on the context. We are required to review and refresh consent if and when appropriate. Explicit Consent can be withdrawn at any time, data subjects must be told how and it must be simple to do (refer to Privacy Notice).

Aside from authorising the collection of Sensitive Data, Explicit Consent can also be used to authorise the transfer of personal data overseas; more specifically, data transferred to a country or territory outside of the UK and EEA not approved by the UK Government as having adequate protection.

Explicit Consent is PIL's only lawful grounds for processing Sensitive Data except in exceptional circumstances, see immediately below.

8.6 Vital interests of a data subject where they are incapable of giving explicit consent

This will only apply when you need to process sensitive personal data but the individual is incapable of giving explicit consent to the processing. In this situation Explicit Consent will not be required as the client would need to be able to fully understand what they were agreeing to. Explicit Consent must only be sought from someone who is capable of giving it.

If processing the data is necessary to protect the vital interest of the data subject then it can go ahead without their explicit consent but a record must be kept of the decision complete with reasons why.

If a client is assessed as being vulnerable, has an attorney but is still capable, interested and participates fully in the advisory process the client must still give their Explicit Consent but the attorney must be present as a witness.

If you have any doubts, please refer them to the Compliance Manager.

## 10. Data Subject Rights

10.1 The right to be informed

PIL is obligated to provide 'fair processing information' typically through a Privacy Notice. Ideally a Privacy Notice should be issued to all clients at the outset of the sales process, prior to the collection of personal data and be issued alongside the Client Agreement.

If you are contacted 'out of the blue' by a potential client and they divulge personal data you should send them a copy of the Privacy Notice in your reply or immediately after the conversation has ended.

A Privacy Notice should be issued to those applying to join PIL at the very start of the recruitment process, when contact is first made.

At its core the Privacy notice must inform the reader:

- who we are;
- what we are going to do with their information; and
- who it will be shared with.

The information within the Privacy Notice must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

10.2 The right of access

Individuals will have the right to obtain confirmation that their data is being processed AND access their personal data. There is no charge for this and the information requested must be provided within 1 month.

10.3 The right to rectification

Individuals have the right to have their personal data rectified if inaccurate or incomplete. We will have 1 month to respond if such a request is made. We are also required to update any third party (if applicable) to whom we have passed their information of the change and inform the data subject who we have updated.

10.4 The right to erasure

'The right to be forgotten'. Individuals have the right to request the deletion of their personal data. This request can be refused providing we have grounds. PIL will either cite legal & regulatory obligation or Legitimate Interests - to defend against a potential claim in the future.

Requests received from clients to whom we have given advice in the past will ordinarily be refused. The personal data of clients who have never received advice from PIL must be deleted after 12 months. Clients falling into this category must be identified and their data deleted by the relevant practices.

Requests from members of PIL, past as well as present will be refused on the basis of legitimate interests. Personal data belonging to un-successful applicants must be deleted after 12 months unless there are exceptional circumstances.

Regardless of the decision, we will have 1 month to respond to the data subject.

10.5 The right to data portability

Individuals have the right obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. This must be provided in a structured, commonly used and machine-readable form within 1 month.

10.6 The right to object

The right to object only applies in certain circumstances. Whether it applies depends on the purposes and the lawful basis for processing. Individuals have the right to object to and stop us processing their personal data where it is being processed using 'legitimate interests'. The data processing activities we carry out under this basis are issuing Newsletters, Recruitment, indefinite file retention and sending mortgage rate renewal reminders.

Clients have the right to object to their data being used for marketing purposes which includes Newsletters and mortgage rate renewal reminders. This is an absolute right and there are no exemptions or grounds for us to refuse.

Objections raised by an individual applying to be a member of PIL will be handled by explaining our reasons for processing their data in the hope that they will withdraw their objections. Where the individual still objects we will uphold their decision and stop processing the data but this will potentially have an impact on the decision whether to let them join the group.

The objections of an existing member can be addressed by explaining the reasons as above but where they persist we can continue processing their data providing that we have established compelling legitimate grounds which overrides the interests, rights and freedoms of the individual or if the data is being processed under other lawful grounds.

Objections by clients denied the right to be forgotten will be refused where they have received advice, only those who have not received advice will have their objection upheld. Objections by past and present members of PIL and unsuccessful applicants will be refused in all instances. We can claim that this is necessary for the establishment, exercise or defence of legal claims.

We have one calendar month to respond to an objection.

## 11. Data Protection Impact Assessments (DPIA)

11.1 A DPIA is a process designed to help identify and minimise the data protection risks of a project. We are required to complete one for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing.

11.2 Having gone through the ICO list of processing types the closest we come to processing data requiring a DPIA is 'processing genetic data'.

11.3 The GDPR defines Genetic data as:

*'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question; and*

*Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.*

11.4 We do not process personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample; at least not first-hand. We do sometimes ask data subjects applying for a product that requires medical underwriting if there is a history of certain medical conditions in their family.

11.5 Medical history, whilst deemed to be special category or sensitive data, does not require a DPIA. For this reason, a DPIA will not be carried out at this time but the situation will be monitored on an ongoing basis and if it becomes necessary one will be done.

## 12. Direct Marketing

12.1 Without client consent the only lawful grounds left open to us if we wish to process client data for marketing purposes is Legitimate Interests. A Legitimate Interests Assessment has been completed enabling us to send clients Newsletters on the grounds that this is in their interests as much as ours but the client retains the absolute right to object. Where this right is invoked we must stop processing their data in this way immediately.

12.2 Where the client objects this must be recorded either on IO or by some other means. They must also be removed from mailing lists so ensuring that that they never receive any other piece of marketing in the future. This record should be kept at a local level, by each office, and kept up to date. Where Head Office receives these objections, the relevant office will be informed.

12.3 Other forms of marketing such as mailshots about certain products and funds will require Consent from the client unless it is included within correspondence not deemed to be marketing such as correspondence linked to advice or an ongoing serving you are contractually obliged to provide. If you do this then you must make sure that you refer to your record of those clients who have objected earlier before sending the material.

## 13. Business/Corporate Clients

13.1 We act as a data processor rather than a data controller in respect of our relationship with businesses and their employees. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller.

13.2 A Privacy Notice has been prepared with this is mind. It reflects the relationship between us and our client (Employer) and their employees who are the data subjects who own the data and have the rights.

13.3 As with all Privacy Notice they should be issued at the earliest opportunity, preferably at first contact.

## 14. Recruitment

14.1 The lawful grounds under which we process the personal data of new joiners are Legal Obligations and Legitimate Interests. For existing members, the same grounds will apply but Performance of Contract will also apply in some circumstances.

14.2 Establishing the data subject's identity, right to work in the UK, Fitness and Propriety assessments and qualifications and experience for advisory members come under Lawful Obligations, everything else is processed as Legitimate Interests. For existing members some data will need to be processed in order to fulfil contractual obligations such as absence records.

14.3 Fitness & Propriety checks entail a Criminal Record check which will require us to obtain Explicit Consent from the applicant/adviser before a check can be run. The applicant/adviser will be asked to complete and sign the Sterling BackCheck form giving consent for this to be done.

14.4 As with all Privacy Notices they should be issued to the data subject at the earliest opportunity, preferably on first contact with a candidate.

## 15. Data Retention

15.1 Individuals have the right to be forgotten. However, there are two lawful grounds available that will serve as an exemption enabling us to deny such a request.

15.2 In respect of clients there are legal and regulatory obligations that state stipulate minimum indefinite record retention periods for certain types of advice and transactions. For everything else we can cite Legitimate Interests and the need to defend against potential legal claims. In the absence of a long stop for complaints we need to be able to process client data indefinitely; where advice has been given. Where advice has not been given, it must be deleted on request or within 12 months of last contact.

15.3 Requests by past and present members of PIL will be refused in all instances, again citing Legitimate Interests as our lawful grounds and the need to defend against potential legal claims in the future or Legal/Regulatory Obligations where appropriate. Personal data belonging to unsuccessful applicants must be deleted after 12 months.

## 16. Privacy Notices

16.1 Privacy Notices must be issued to clients, potential clients or new members of PIL at **the earliest opportunity.** This requirement stems the Data Subject's right to be informed. We are obligated to provide 'fair processing information'. We should not collect and process personal data until this has been issued if it can be avoided.

16.2 We have 3 types of Privacy Notice, one version is for Private Clients, another is for Business/Corporate Clients and the last is for those applying to join PIL and current members. All are located within the appendices of this document.

16.3 A Privacy Notice must be issued to clients at the first point of contact and typically at the same time as the Client Agreement. A Privacy Notice must be issued to potential members of PIL at the first point of contact. A Privacy Notice should be issued by business owners to those members who works for them the next time collect data from them but they are available on request.

16.4 A Privacy Notice should be signed in order to evidence that the individual concerned has received and read it.

16.5 Privacy Notices contain an Explicit Consent statement giving us the right to collect and process Special Category data if it becomes necessary (medical underwriting). Explicit consent is obtained when the data subject signs the Privacy Notice. **You cannot collect or process this type of data until you have obtained this consent.** In addition, the privacy notice can be used to obtain Explicit Consent for international data transfers into jurisdictions not recognised by the UK Government as having adequate protection in place.

16.6 Obtaining Explicit Consent may not turn out to be necessary but it is better to get this in advance rather than run the risk of forgetting to obtain it later on when it is necessary. Having consent does not mean that we need to make use of it unnecessarily. We must not collect or process Special Category (Sensitive Data) unless it is necessary, e.g. to take out a life assurance policy or join a Group Medical Scheme where this data is required for underwriting purposes.

16.7 Privacy notices only need to be reissued if the one issued previously has been replaced with a newer version, much like the Client Agreement.

16.8 We are not obligated to do anything for those clients with whom we have had no contact since before the implementation of the GDPR in 2018. Our Privacy Notice is available on the PIL website. The appropriate Privacy Notice can be given to former members of PIL on request.

## 17. International Data Transfers

17.1 There are strict limitations on when personal data can be transferred outside of the United Kingdom. When procuring IT services, we must establish where in the world the data will be processed – are the servers outside of the UK?

17.2 Following the UK's departure from the EU, there was mutual recognition of each other's data protection rules. Both sides have decided that each other's regimes offer adequate protection. As a result, there are no restrictions on the transfer of personal data to EEA countries. These are as follows:

| | | |
|---|---|---|
| Austria | Germany | Malta |
| Belgium | Greece | Netherlands |
| Bulgaria | Hungary | Norway |
| Croatia | Iceland | Poland |
| Cyprus | Ireland | Portugal |
| Czech Republic | Italy | Romania |
| Denmark | Latvia | Slovakia |
| Estonia | Liechtenstein | Slovenia |
| Finland | Lithuania | Spain |
| France | Luxembourg | Sweden |

17.3 The European Commission recognise that certain countries and territories provide adequate protection for the rights and freedoms of data subjects in connection with the processing of personal data. The countries holding this status at the point the UK left the EU on 31/12/20 were recognised by the UK Government as offering adequate protection. These countries are as follows:

| | | |
|---|---|---|
| Andorra | Guernsey | New Zealand |
| Argentina | Isle of Man | Switzerland |
| Faroe Islands | Israel | Uruguay |
| | Jersey | |

17.4 Since leaving the EU, the UK had made its own 'adequacy decisions' to include Gibraltar and Japan. In the case of Japan this only cover private sector organisations.

17.5 Personal data can still be sent to an unapproved country, territory or organisation outside of the UK providing we can:

- assess adequacy;
- use contracts, including the ICO approved model contractual clauses;
- get our Binding Corporate Rules or Binding Corporate Rules for Processors approved by the Information Commissioner; **or**
- rely on the exceptions from the rule.

17.6 Where one of the conditions listed in 17.5 cannot be satisfied the only option left is to request Explicit Consent from the data subject.

17.7 Currently, we transfer personal data to only two firms based in a country not deemed to offer adequate protection, at this time, by the UK Government. The country in question is the USA. The Cognito Forms Mortgage Factfind cannot be completed unless the client/s give Explicit Consent at the beginning. The practice that uses Dropbox to store client files has a slightly amended Privacy Notice which obtains the required Explicit Consent when signed by the clients.

## 18. Website Cookies

18.1 A cookie is a small file of letters and numbers that is downloaded on to a computer when visiting a website. Cookies are used by many websites and can do a number of things, e.g. remembering preferences, recording what has been put in a shopping basket, and counting the number of people looking at a website.

18.2 Where cookies are used on any websites used by PIL and its member to promote our services you must ensure that a pop-up warning advises visitors of the following:

- That cookies are used.
- What cookies are and what they do.
- The importance of necessary Cookies and an option to deselect cookies that are not necessary.
- Obtain Consent.
- Inform the visitor of their ability to manage cookies through their internet browser.

## 19. Data Security

19.1 Under the rules we are required to protect the personal data we process from unauthorised or unlawful processing and from accidental loss, destruction or damage, using appropriate technical or organisational measures.

19.2 IT equipment, which is Desktop and Laptop PC's and network severs must have the following in place to fulfil this obligation:

- Firewall
- Anti-Viral/Malware/Ransomware software
- The software for the above must be regularly updated
- Anti-Viral/Malware/Ransomware scans must be run on a regular basis

- Microsoft updates, in particular security updates, must be run on a regular basis
- Backed up data stored locally on portable l Hard Drives must be stored securely.
- Personal data backed up using a cloud solution must be encrypted in transit and 'at rest'

Updates must be run automatically on weekly basis to minimise the risk of a breach.

## 20. Secure Emails

20.1 Keeping personal data secure does not begin or end with protecting data stored on office IT Equipment, it also bears consideration when in transit. When sending personal data by email we must consider using a secure and encrypted email system or an online portal that allows documents and messages to be uploaded/sent and downloaded/received with encryption at both ends.

20.2 Any email contains enough personal data to enable a third party to steal the data subject's identity and ALL data classified as Special Category (Sensitive) is **best** sent securely.

20.3 Data required to steal a person's identity is as follows:

- Full name
- DOB
- Current and previous addresses
- Place of birth
- Mother's Maiden name.

20.4 Items that should typically be emailed securely are as follows:

- Emails containing the above information
- Factfinds
- Suitability Reports
- Applications forms
- Legal documents such as Lasting Power of Attorney.

20.5 Before requesting, receiving or sending any of the above data and items by standard email you should give the data subject the **option** of using an alternative and act according to their wishes.

20.6 You should advise them of the advantages but also the disadvantages attached with more secure methods of communication. The dis-advantages include the extra layer of complexity associated with creating a password and remembering it later. In respect of secure emails, lenders and providers may not receive them or if they do, they may be unable to open them owing to the security systems they have in place at their end.

20.7 If the data subject has reservations about secure email or online portals for the reasons above, amongst others, you should confirm if they are happy for the data and items above to be sent and received within PIL, between us and them, and between us and the provider/lender by standard email which is not secure. **Client responses should be recorded on their file.**

20.8 All members of PIL should offer data subjects the option of sending their personal data securely with emails being encrypted in transit and 'at rest' (destination).

## 21. Data Processors

21.1 The rules require Data Processors to conform with Article 28 of the GDPR and Controllers have an obligation to ensure that they do.

21.2 Data Processors are third parties to whom we pass on personal data. This is done so that the data processor can provide us with a service. The services they provide are essential to the smooth running of our business and aid us in providing the advice and services we are contractually obliged to give our clients. They can also help us fulfil our legal and regulatory obligations.

21.3 A list of PIL's Data Processors is as follows:

| | | |
|---|---|---|
| Intelligent Office | Smartsearch | Trigold/XPLAN Mortgage |
| Volume | Genovo | The Exchange |
| Dropbox | Selectapension | Assureweb/Solutionbuilder |
| Cognito | O&M | Acronis |
| Cash Calc | Mortgage Brain | RISC |
| FE Analytics | Twenty7Tec | Sterling Backcheck |
| Adviser Asset | Underwrite Me | Mortgage Broker Tools |

**This is not a static list and will change over time**

21.4 The above firms have been contacted and all have confirmed that they are compliant with the GDPR. They have sent either a revised terms and conditions, contractual agreement or an addendum to the existing one covering off the requirements in the GDPR. For more information on what was asked of them and what has been provided please find the Third-Party Record in the appendix.

21.5 We are required to keep a record of all T&C's/contractual agreements, revised versions and addendums existing between ourselves and our data processors. These records are updated on an ongoing basis.

## 22. Cyber Insurance

22.1 Cyber and data risks insurance is designed to support and protect us against a data breach and an attack by a malicious hacker.

22.2 We have taken up this insurance and it will cover us for the following:

- Cyber Crime
- System damage and business interruption
- Network Security & Privacy Liability
- Court Attendance Costs

22.3 The policy has a variable indemnity limit up to a maximum £500,000 for both single and aggregate claims over a 12-month period.

## 23. Breach Notification & Penalties

23.1 We have a duty to report certain types of data breach to the ICO and in some cases to the individual affected.

23.2 A personal data breach is defined as a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data!

23.3 We are only required to notify the ICO of a breach where it is **likely** to result in the rights and freedoms of the data subject being put at risk. Where a potentially reportable breach has occurred, the Compliance Manager must be informed. The Compliance Manager will refer the matter to the board and the board will decide if the breach is reportable.

23.4 Where a breach is deemed likely to result in a high risk to the rights and freedoms of individuals the ICO will be informed. **Notifications must be made within 72 hours of becoming aware of the breach.**

23.5 We must notify the data subject concerned directly without undue delay.

23.6 The penalties for non-compliance with the GDPR can be severe; these can include a ban on processing, withdrawal of certification and fines of up to 4% of annual turnover. Non-compliance could also constitute a breach of Systems & Controls requirements and could attract FCA disciplinary action.

## 24. Staff Training

24.1 All new members of PIL receive training on induction. Existing members will receive refresher training on a bi-annual basis.

24.2 All members of PIL have signed a declaration confirming that they understand their responsibilities and obligations laid down in the Data Protection training slides and in this policy. This exercise will be repeated after each refresher training event.

## 25. Compliance Monitoring

25.1 Compliance with the rules will be monitored in the course of regular new business file checks. In particular monitoring will focus on whether the GDPR principles are being adhered to.

25.2 Specifically, the things that will be looked for are as follows:

- That a Privacy Notice has been issued to clients at the earliest opportunity.

- That the personal data collected is relevant and limited to what is necessary. Sensitive data must not be collected unless absolutely required and not before Explicit Consent has been obtained from the client.
- That the data collected is consistently correct throughout the client file and that any request by a client to amend their personal data is completed within the stipulated time frame of month.
- That Secure Emails are used when appropriate to keep Personal data secure in transit and 'at rest'.

25.3 Compliance document templates will be reviewed on a regular basis to ensure that they do not prompt clients to provide us with personal data that is not strictly to provide the advice and service required of us by the client.

## 26. Appendixes

- Privacy Notices
- Client Agreements
- Factfinds
- Legitimate Interests Assessments (LIA) x 4
- Third Party Record