DATA PROTECTION POLICY

OF

S&S Heffernan Limited

November 2024

Introduction

S&S Heffernan Limited principal business is to provide advice and arrange transactions for our clients in relation to life assurance, pensions and Insurance based Investments and we have an agency with. This document outlines how we treat clients' personal data and how we adhere to the Data Protection Regulations.

TABLE OF CONTENTS

1. Data Protection Principles

Process data (information) fairly.
When collecting or recording data, we clearly identify our business and address, we Identify the purpose for collecting the data and to whom the data is disclosed (insurers, others).

Collect data for one or more specified, explicit, and legitimate purposes and use it only in ways which are compatible with those purposes.
The data provided to us will only be used for the purposes as clearly stated to our customers. Customers are given the option to consent to non-essential uses such as marketing or profiling for marketing purposes.

Ensure that data is adequate, relevant, and not excessive in relation to the purpose(s) for which it was collected.
Customers will not be asked for information that is not needed for the stated purpose. Where there is either a legal/regulatory requirement or a legitimate business need to hold data. Once collected, only the minimum data that is needed for a particular purpose is used/disclosed (known as "data minimisation").

Keep data accurate and, where necessary, up-to-date and take all reasonable steps to erase or correct inaccurate data.
We ensure that customers' data is updated promptly when notifications are received.

Retain data for no longer than is necessary for the specified purpose(s).
We are required to keep client's data for at least 6 years after the relationship with our clients ends, this is a requirement of the Central Bank. After this time, we destroy the data securely e.g., by confidential shredding.

Keep data safe and secure including taking appropriate technical or organisational measures against unauthorised access, alteration, disclosure, accidental loss, or destruction of the data.
We use the IT services which are detailed further in this document for our client's database and storing of documents, we have a term of agreement with these providers. The agreement covers the safe security of our data and full back-up procedure in the event of a system failure in our office.
Our pcs and laptops are password protected, and all data is held in the cloud.
Our email system is held securely.

Accountability: the business is accountable for all the above principles and ensures the business is GDPR compliant.

2. Data Protection Officer

We do not have an appointed data protection officer as we do not process data on a large scale, where the core activities of the organisation (controller or processor) consist of data processing operations, which require regular and systematic monitoring of individuals on a large scale; or we do not process Sensitive/special category data: Where the core activities of the organisation consist of special categories of data (i.e. health data) or personal data relating to criminal convictions or offences. However, we do have one person who is responsible for all areas of data protection and ensuring we are compliant with the rules. This person is Stephen Heffernan.

3. The Grounds for Data Processing

- **We** have a legal basis for processing each type of personal data we hold, see separate analysis on data held file.
- We ensure one of the following grounds are satisfied to process Personal Data: -
- **Consent** - Consent of the data subject
- **Contract** - Necessary for the performance of the contract

- **Legal Obligation** - Necessary to comply with a legal obligation.
- **Vital Interests** - Necessary to protect the vital interests of the data subject.
- **Legitimate Interests** - Necessary for the legitimate interests of the data controller, unless such interests are overridden by the interests of the data.
- **In the case of Criminal History/ongoing criminal proceedings only: Risk Assessment or Fraud Prevention.** Note: Criminal history is no longer deemed Sensitive (or Special Category) data.

Legitimate Interests may be an appropriate ground when if we wish to process data in a new way (e.g. implement a new Group-wide CRM system which would mean greater efficiency in sharing customer MIS with other Group companies but would also mean increased access to customer data and increased security risks) for its own legitimate commercial reasons but where there is no legal ground to rely on and there is no realistic prospect of obtaining the consent of every customer or every staff member as the case may be.

To rely on Legitimate Interests as a legal basis for processing personal data, we will Inform data subjects in our Privacy Policy of both the processing and the Legitimate Interests for it plus their right to object (on "compelling legitimate grounds" only); and
Carry out an assessment and document our rationale, including the safeguards in place for data subjects. When doing so, consider the actual effect of the processing on individuals, i.e., rather than an academic or abstract exercise; and Keep documentation available for inspection by the DPC.

<u>The Legitimate Interests Assessment will include the following: -</u>

- The rationale for relying on Legitimate Interests and why the other grounds are not appropriate.
- A description of our Legitimate Interests (e.g., the commercial benefits) and the factors that make these Interests (i) Lawful; (ii) Concrete; and (iii) Real and tangible i.e., not speculative.
- An assessment of the necessity of the processing, i.e., setting out the alternatives that have been considered and whether there are any less invasive options available.
- A provisional assessment as to whether our Interests are overridden by the rights of the data subject(s), taking into account:
- The possible prejudice if the proposed process does not go ahead (or continue).
- The nature of the data involved.
- The status of the data subject(s) relative to that of our firm (is it unequal?).
- The way the data is processed and the impact on the data subject(s).
- The data subject's reasonable expectations.
- The impact versus the benefits of the processing; and
- A final assessment taking account of additional safeguards, such as:
- Data minimisation: e.g., strict limitations on the data collected, immediate deletion of data after use.
- Technical and organisational measures to ensure that the data cannot be used to take actions or make decisions about the data subject(s) ("functional separation").

Increased transparency, right to opt out, data access and data portability rights available to the data subject(s).
We will not transfer personal data outside the EU/EEA unless it meets the requirement of the EU data Protection legislation.

4. Legal Bases for Processing - Sensitive/Special Category Data (e.g. Health data}

We satisfy the following to process Sensitive Data: -

- **Explicit Consent** - Explicit consent of the data subject
- **Vital Interests** - Necessary to protect the vital interests of the data subject where the data subject is incapable of giving consent.
- **Insurance and Pension purposes** - Necessary and proportionate for the purposes of providing an insurance, pension, or mortgage product.
- **Legal Obligations under Employment Law/Social Welfare Law** - Necessary for carrying out either the obligations of the employer or for exercising the rights of the employer or employee.
- **Medical Assessment/Diagnosis/Treatment** - Necessary for the purposes of preventative/occupational medicine, the assessment of the working capacity of an employee,

medical diagnosis.
- **Legal Advice and Legal Proceedings** - Necessary for obtaining legal advice whether in the context of a claim (or prospective claim).

5. Conditions of Consent

- **Positive Action** - Clear affirmative action is required, no pre-ticked boxes, no implied or assumed consent in the event of no positive action by the data subject.
- **Free will** - Will be freely given, so will not be appropriate where (i) the processing is necessary to perform the contract (or to provide the product), or (ii) where there is no real free will, for example as between employee and employer: Legitimate Interests or Employment Law obligations may be a more appropriate ground.
- **Specific** - Will be specific to the options given, so for example a customer will be able, should they wish to, withhold their consent to Profiling for Marketing purposes but to consent to Marketing itself. So, when consent is requested in the form of a written declaration, then the different options will be set out individually and separate consents requested for each option, and in an intelligible easily accessible format using clear and plain language.
- **Recorded** - Will be verifiable, a record will be kept of how and when consent was given. So, consent can be confirmed over the phone if calls are recorded. We will ask a customer to sign acknowledgement on our terms of business for marketing and profiling purposes.
- **Withdraw consent.**

We will inform our clients of our terms of business and of the privacy notice of their right to withdraw their consent at any time.

6. Privacy Notices

Our Privacy Notices will contain the following information:
- The firm's name and contact details.
- The DPO's contact details.
- The different types and categories of personal data are held.
- The purpose of the processing and the legal basis for the processing.
- Where this ground is relied upon: Our legitimate interests and an explanation of those interests.
- The recipients or categories of recipients to whom data is shared/disclosed.
- Details of any transfers outside the EEA, the safeguards in place and how to obtain a copy of them.
- The data retention period or the criteria used to determine the data retention period.
- The individual's rights include: the right of access to data, rectification and erasure, restriction of processing, objection to processing, data portability.
- Where the processing is based on Consent, the right to withdraw consent at any time.
- The right to complain to the DPC.
- Details of any automated decision-making including profiling, and the logic involved as well as the significance and consequence for the individual.
- Whether the requirement to provide the data by the individual is a statutory or contractual obligation and the consequences of failing to provide the data.

A vital part of GDPR compliance is communicating with our clients. Explaining exactly how and why we are collecting their personal data and indeed, what we intend to do with it.

7. Data Subject Rights & Requests: Access, Portability, Rectification, Erasure

Individuals (customers and staff) are entitled to avail themselves of certain rights conferred under the Data Protection Act. These are outlined in turn as follows.

Right of Access
The most significant of these rights is the individual's right to access their personal data. Such requests are known as "Data Access Requests" or Subject Access Requests".

The format of the Request: -

- It must be in writing, but this can include email, fax and even text message.
- It must provide relevant details needed to help identify the individual and to locate the required information (so at the very least name and policy number).
- It does not have to refer to the Data Protection Act; it can simply state that the individual requests a copy of their data held by us.
- Template Request forms will be used but are not mandatory. While an individual is entitled to copies of all information held about them, forms can help greatly in encouraging individuals to be specific about what they are looking for. Very often a quick phone call can save time. We will not charge for a data request.

Data Access Request Form, refer to Appendix 1

Timeframe for responding to data requests
We will reply with the information requested within one month of receiving the request and once satisfied of the individual's identity - or up to a maximum of 3 months for complex cases: we will inform the individual of the need for the extended period and will provide as much of the data as possible in the meantime. We will confirm identity by requesting the client's date of birth and their address.

Format of Response: -

- We will include a copy of the data in an intelligible form i.e. photocopies will be legible, abbreviations explained.
- We will provide by email if the request is received by email, unless otherwise requested.
- We will inform the individual if no information is held about them.
- We will inform the individual if their right of access is restricted and be told of their right to complain to the DPC about the refusal.

Grounds for restricting or refusing access
There are limited grounds for restricting or refusing a data subject access request. The grounds available are: -

- Legal Privilege - This ground has been broadened by GDPR and covers all communications between us (the data controller) and their legal advisors (internal/external) regardless of whether legal action is likely or anticipated.
- Third Party data - References identifying other (third) parties, for example the names of other customers, will be removed (redacted). However, references to staff who would be known to the customer (e.g. the staff member who the customer has dealt with) should be retained.

- Opinions given in Confidence - References to third parties (e.g. Individuals in previous employers) who have given Employment References in confidence will be redacted.
- Similarly references to the identity of whistle-blowers or witnesses in an internal investigation will be redacted unless consent has been given.

Ongoing Criminal or internal misconduct investigation

- Data can and will be withheld where there is an ongoing Gardai investigation concerning the individual (e.g. fraud by a customer) or where misconduct suspicions/allegations concerning a staff member are being monitored/investigated.
- When replying to any Access Request in such circumstances, these grounds must not of course be mentioned.

Commercially sensitive data

- Any data which may be commercially damaging or disadvantageous if known to our competitors or customers can be removed.

Health data were harmful

- Health data will be removed where, in the opinion of a medical professional, to do so would likely cause serious mental or physical harm to the individual.

Example: A medical report obtained by an employer to assess an employee's readiness to return to work following a long period of sick leave. When replying to any Access Request in such circumstances, these grounds will not of course be mentioned.

Disproportionate effort

- Where we can legitimately argue that to respond to a Request would take an unreasonable amount of time and effort (much more than the average Request would take), and certainly more than 90 calendar days, then this ground can be availed of.
- However, all reasonable efforts will be made to identify what in particular the individual is looking for and, in any case, to provide the individual with at least that which is possible within the 90-calendar day timeframe.

Best practice

- We will inform the individual that a certain amount of the data (give some detail) can be provided within a certain timeframe and the remaining data (again give some detail) within a further specified time.

Repeat requests

- We are entitled to refuse to respond to repeated requests within timeframes where in those timeframes the data is unlikely to have changed. Where a follow-up request is made, it is sufficient to provide the individual with the updated data only since the previous request.
- If more than 1 request is made in any 12-month period, we will only provide the client with the information that has changed since the last request.

Requests from third parties on behalf of the individual

Care must be taken when considering requests stated to be made on an individual's behalf e.g. by advisors. The following is our practice: -

- Legal advisors. A solicitor's letter on headed paper can be actioned as it is, even without an individual's signed authority.
- Powers of Attorney. Can be actioned with copy of power of attorney on file and checking the person we are talking to has the power.
- Financial advisors. Either an individual's signed authority must be included or already on file.
- Family members or acquaintances. Must be refused with or without the individual's authority.

However, Data Protection does not affect dealing with operational requests in the usual way. Public representatives will be refused with or without the individual's authority.

Defamatory data

The fact that data includes inappropriate comments is not a ground for redacting that data. Data cannot be cleansed of defamatory statements or harmful content once the request has been obtained. We ensure our staff should be reminded of the need to be careful about recording any subjective comments about an individual and that all comments recorded should be factual in nature.

Record keeping

We keep a copy (scanned preferably) of the response provided, in the event of a query or complaint.

Enforced Access Requests

It is illegal to force an individual to make an Access Request. Examples: A prospective employer cannot request or ask (effectively forcing) a job applicant to make a request from their current/previous employer. A car insurance applicant cannot be forced to allow their details to be disclosed by the NVDF (the National Vehicle Driver File).

Right of Data Portability

Our customers have the right to receive their data, not in hard copy or by email as a subject access request but on a form in which they the customer can use it and re-use it electronically as they wish.

So, they can request that their data be so-called "ported" either to themselves or to another Broker.

Key features are as follows: - Only the following data is covered.

- The data provided to us by the individual themselves. And any observed data (e.g. transaction

history, access log).
- Excludes paper files.
- Excludes data provided to comply with a legal obligation e.g., AML data.
- Excludes staff data where required for employment law
- Excludes data produced by subsequent analysis of data provided by the individual, i.e. inferred or derived data (e.g. risk scores).

Format
Will be secure and we will allow the data to be used and re-used (i.e., in an interoperable, machine-readable format) from the supplier we have our database with.

Timeframe
One calendar month - or up to three calendar months for complex cases and where the individual has been informed of the reasons for the extended time period.

Right of Rectification
Individuals have a right to have their data rectified or corrected - but only where the individual informs us of an error in their basic personal or contact details.

Right to have processing restricted or stopped
Individuals may request us to stop their data being used for certain purposes e.g., for direct marketing. This is in effect the equivalent of an optout request and will be recorded on our system. Our direct marketing declaration is on our terms of business which is given to each client and signed or replied to on email to confirm direct marketing is consented to.

Right of Erasure & Right to be Forgotten
Individuals have a right to have their data erased or deleted where the data has been held for longer than necessary or if the processing is not in compliance with regulation - but not where the data has been held correctly in accordance with our Retention Schedule.

Right to Complain to the DPC
If a client is dissatisfied with the way, we handle their Personal Data they can contact us. We will do our best to address their concerns swiftly and resolve any issues they have. They have the right to complain to the Office of The Data Protection Commission, Canal House, Station Road, Portarlington, Co. Laois, R32 AP23. www.dataprotection.ie Tel.: +353 (0)761 104 800. Fax: +353 57 868 4757. E-Mail: info@dataprotection.ie

Right to Sue the Controller and Processor
New statutory right to damages - now even in cases of non-material loss.
Individuals are able to claim damages for breaches of Data Protection in respect of their personal data - even where no loss or damage has resulted.

8. Automated Decision-Making & Profiling

Automated decision-making and Profiling are techniques often used in the financial services sector to both streamline processes and to measure risks or identify opportunities.
An automated decision is one that: -
- Concerns an individual.

- Uses that individual's personal data.
- Is made entirely without human intervention; and
- Has important consequences for the individual (i.e. either "legal or similarly significant effects"). E.g. - The giving of quotes and indicative quotes on-line

We inform clients on the terms of business and on the privacy notice that an Automated Decision-Making process is involved; Following the quote, the right to have that quote reviewed by a sufficiently senior member of staff.

Profiling
Profiling is defined as "Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."
So, Profiling is any kind of automated processing which uses personal data to analyse or predict certain characteristics or preferences of an individual(s). E.g. Profiling for Marketing purposes - Risk assessments for fraud prevention/AML purposes. We inform clients and get their consent to use profiling on their data.

In certain cases (only), the individual also has the right to object/opt out of such Profiling. These are where the Profiling is: -Not required for the performance of the contract (i.e. to provide the insurance product); OR Not required for any legal or regulatory reasons.

9. Direct Marketing

Data Protection imposes strict obligations on the use of personal data for direct marketing purposes. These are in addition to obligations required for example by the Central Bank of Ireland and should be read as such. It is commonly but mistakenly thought that because GDPR requires Consent to be a positive action that this means that all Marketing preferences must now opt In. This is not the case. GDPR makes no changes to the current Marketing rules. GDPR does however recognise Marketing as a Legitimate business activity.

Post
- We tell our customers (or potential customers) that we intend to use their data for marketing purposes and give them an opportunity at point of collection to refuse such use or **opt out** (for example, we provide an opt in "tick-box" on our terms of business).
- An individual may withdraw consent to direct marketing at any time.
- We have 28 days to comply with a request to cease direct marketing.
- For non-customers, we can use names and addresses on the most up-to-date version of the Edited Electoral Register but not the Full Register for postal marketing. Individuals on the Edited Register are those who, when registering to vote, did not object to personal data being used for marketing.

Telephone
- We tell our customers (or potential customers) that we intend to use their data for marketing purposes and give them an opportunity at point of collection to refuse such use or **opt out** (for example, we provide an opt in "tick-box" on our terms of business).
- In the case of a **customer,** we can call them even if they have opted out from receiving marketing calls on the National Directory Database ("NOD"), i.e. the consent given to our firm outweighs the preferences recorded on the NOD and so we do not need to check the NOD.
- However, in the case of a **non-customer,** we will check the NOD for any optouts recorded before calling that individual, i.e. the NOD opts out will override any consent given to our firm.

SMS Messages
SMS messages are considered like email and the same rules apply.

Email - individuals and business customers
At the point of sale, we tell our customers that we intend to use their data for marketing purposes and give them an opportunity at point of collection to refuse such use or **opt out** (for example, we provide an opt in "tick-box" on our terms of business after that all marketing that goes to clients will give them the option to

opt out).
For those customers who opt In, we email them for marketing purposes, so long as: -

- It is within 12 months of the initial point of sale and receipt of their email details.
- The product or service being marketed is our own.
- The product or service being marketed is similar to that supplied to the customer in the context of the (previous) sale (e.g. another insurance product).
- In the email (and all subsequent emails), the customer is given a clear optout not to receive further such emails.
- All subsequent marketing emails are within 12 months of the previous email and the customer has not opted out since the last email.

Email - non-customers
For non-Business non-customers**:** We will have their prior explicit consent (i.e. **opt in)** before emailing them for marketing purposes.
However, for Business non-customers (even individuals, sole traders for example) - we can email them for marketing purposes as long as their business or official email is received by us in the context of commercial or official activity or is listed in a Business Directory.

Buying in Marketing Lists

- We may buy leads lists from marketing companies, but we confirm that their consents are explicit by checking them first against our own system for any preferences indicated to our firm and then against the National Directory Database (for phone) and Electoral Register (for post).
- More generally: -
- We will only use reliable marketing firms; do our research and check customer complaints.
- We will have a contract in place with the marketing firm which requires them to be DP and GDPR compliant.
- When we market to the leads on the list, we will refer to the name of the marketing firm as our source for their contact details.

10. Data Breach Reporting & Security

In the event of a data breach, we will do the following.

- Without undue delay and no later than 72 hours of becoming aware of the breach; Where there is a risk to the rights of the data subject(s), i.e. Where the security of the data has been compromised or where the risk has not been contained in some way e.g. by encryption; and taking account of the likely impact on the data subject(s); but Regardless of the sensitivity of the data.
- We will make all reasonable efforts to secure the data in a timely manner.
- Practical examples:
    - Mailing label error: The customer's correspondence is received by a third party and is opened by them. Assuming the third party informs the firm or the customer, then that breach must be reported to the DPC.
    - Note: Postal errors (i.e. errors in delivery by the Postal Service) will not be reportable, nor will mailing address errors where the envelope has been delivered to the correct address unopened i.e. the risk to the data that has been contained.
    - Unencrypted laptop: One of the firm's laptops containing customer data is mislaid and is not encrypted, that breach must be reported to the DPC.
- The breach will be notified to the DPC online.
- The content of the report will contain the following: -
    - A description of the records involved including the type and category of the data.
    - The numbers of data subjects affected.
    - The likely consequences of the breach.
    - The measures taken or planned to be taken to recover/secure the data; and
    - The contact details of the firm's DPO or other contact point in relation to the breach.

We will also notify the data breach to the data subject(s): - In the following cases all cases.

- Only where there is a high risk to the rights of the data subject(s), i.e. Where the security of the data

has been compromised; and
- The data is sufficiently sensitive or financial in nature to likely have serious consequences for the data subject(s); or
- Where the data subject(s) needs to be informed in order to take certain steps to safeguard their data.
- But not where disproportionate effort would be involved, in which case public communication would be more appropriate.
- Practical examples:
    - Mailing label error (above): Where the customer correspondence contains sensitive data, e.g. health details, and is opened by the third-party recipient, then assuming the customer is not already aware, they must be informed.
    - Unencrypted laptop (above): Where the laptop contained customers' bank details and there is a risk to the security of the customers' accounts, then the customers must be informed.
- Without undue delay once becoming aware of the breach (unless on the rare occasion investigating authorities request a delay).

Format & content of notification to the data subject(s): -
- A description of the nature of the breach.
- The name and contact details of our DPO or other contact point in relation to the breach.
- A description of the likely consequences of the breach for that individual; (iv)The measures taken or planned to be taken to recover/secure the data or to mitigate its adverse effects; and
- The specific advice to the data subject(s) to protect their data (e.g. resetting passwords where access credentials have been compromised).

We report Data Breaches to the Central Bank: - Where there's a Cyber Security element to the breach, e.g. hacking into our systems, which could have a significant and adverse effect on our firm's ability to provide adequate services to our customers.

Incident Response Plan
If a staff member is aware of a breach, they must report it to the person in charge of data protection within our business. The breach will be dealt with by that person as above.

Record-keeping
A record will be kept of all data breaches regardless of whether they are reported to the ODPC or not. Best practice: Records of those breaches not reported to the DPC should include the reasons for not reporting. The record must contain details of the breach, the cause, those affected, and the measures taken.

Processors
Where data is processed on our behalf by a Processor, there will be a written contract in place.
The contract will include (i) the data to be processed, the extent and purpose of the processing, the duration of the processing and the means by which the data will be safely returned at the end of the contract; (ii) that the Processor must act only in accordance with our instructions; (iii) the guaranteed safeguards the Processor will put in place in respect of the data; and (iv) the Data Protection and Confidentiality obligations owed by the Processor.

Data Security obligations
- We have in place appropriate security measures for our data software system for our client's data, this system is secure and held in the cloud, it also facilitates a back-up service. There is a term of agreement in place with our supplier. This service is password protected.
- Our email system is secure and robust.
- Our pcs have anti-virus software and are password protected
- All paper files are locked away each evening in cabinets or filing drawers. Our premises have a secure alarm and locking system in place with added security of shutters outside.
- We secure and lock away laptops and other portable equipment and computer media like discs or memory sticks securely at night.
- No files are kept in staff cars unless locked safely in the boot.

11. Business Continuity

In the event of a system failure or damage to PCs or premises, we will be able to facilitate to use of our cloud provider to allow us access to systems from different premises with new IT equipment. This back-up facility will be checked once a year. All contracts with data processors we oblige them to have GDPR-compliant security measures in place and to guarantee GDPR-compliant security standards.

Technical measures to avoid a breach include: -

- Access controls based on job role
- Passwords
- Firewalls and virus protection
- Screensavers
- Security updates
- Anonymisation
- Encryption
- Pseudonymisation (data where the data subject's identity is removed but can be recovered by a code only known or accessible by a limited number of individuals in the firm).
- Securing/locking away paper records locked up at end of working day ("clean desk policy").
- Control of physical access to premises, supervision of visitors or visitors kept only to certain public areas.
- Adequate clauses in third party service provider contracts to ensure that employees, agents, and subcontractors of that third party are aware of what is required to ensure compliance with data protection requirements.
- We disposal of paper waste containing personal information, e.g. by shredding.

12. Data Retention

We only hold personal data for as long as necessary, i.e. For as long as required under legal or regulatory requirements; or for as long as required for legitimate business purposes.

By way of examples: -

- FSPO requirements on long term investment products or mortgages.
- Restrictions on retaining data on Spent convictions (the "7-year rule"); and
- CBI/CPC requirements on retaining Fact Finds.

Documented Retention Schedules setting out the retention periods and their rationale for each category of data is in place see analysis document on “data held” file.

Retention Schedules will be reviewed periodically (best practice: annually) to ensure their completeness.

- Data will be purged/deleted in line with the Retention Schedules and clear responsibility for doing so assigned within to the staff member in charge off data protection.

See “Data Held” breakdown for specific time periods.

13. Data Protection Impact Assessments ("DPIAs")

Data Protection Impact Assessments are assessments carried out to understand the risks associated with a certain aspect of data processing, the privacy impacts on individuals and the controls/safeguards which need to be put in place before implementing that processing.

DPIAs are mandatory for all new processing from 25 May 2018 where: -

- New technology is introduced (e.g. a new CRM system is being developed or customer data is to be outsourced to the Cloud) or existing technology is to be upgraded; or
- Automated decision-making or profiling is involved, e.g. risk scoring or quoting premiums on an automated basis; or
- Systematically monitoring of our employees' activities (e.g. email, internet usage); or

- Processing sensitive personal data on a large scale - e.g. health data or data relating to criminal history; or
- Systematic monitoring of publicly available area(s), e.g. CCTV; or
- Sharing or transfers of personal data outside the EU/EEA even between different companies within the same Group.

DPIAs are in essence like any risk assessment undertaken, they will contain the following: -

- A detailed description of the process.
- A simple data flow diagram which would be understood by the end customer/lay man (comprising data sources, data processes/uses and data disclosures).
- Reference to complying with any approved Industry Code of Conduct (e.g. the Code of Conduct for Data Protection in the Insurance Sector).
- An assessment of the necessity and proportionality of the processing (including any alternatives considered).
- A description of the Data Protection risks and the extent to which they will be managed, i.e. the controls/ mitigants and actions required (if any) for each.
- The extent to which interested parties were consulted (e.g. the DPO, internal stakeholders giving names and job titles, external parties such as suppliers/processors).
- An overall assessment of the Residual Risk to data subjects (customers, employees).
- This will be signed, dated and a copy saved to pdf format for an audit trail.
- If the DPIA shows a High Residual Risk after taking account all controls and mitigants, the proposed processing must be notified to the DPC for its approval.

DPIAs will be made available to the DPC on request.

14. A Record of Processing Activities

Replaces the current system of **Registration with the ODPC.**
Is an internal Record open to inspection by the DPC on request.
Brokers will be required to keep such a Record, even those Brokers with fewer than 250 employees, because the processing by Brokers: -

- Is not occasional or once off; and
- Involves sensitive data including criminal history.

The Record contains the following details: -

- The Broker's name, address and DPO contact details.
- Categories of personal data.
- Categories of data subjects and recipients.
- The type of processing carried out and the purpose(s) of each.
- Retention periods for each category (or reference to a detailed Retention Schedule).
- Any transfers of data outside the EU/EEA and the safeguards in place.
- The technical and organisational security measures in place (again with reference to our firm's Security Policy(ies).

See separate “data held” analysis file.

A Data Log of Automated Processing Systems the Log will contain the following details: -

- The collection of personal data.
- The access to that data by any person, with the date, time, and identity of that person.
- The disclosure or transfer of any of that data to any person, with the date, time, and identity of that person.
- The combination of that data with any other data; and
- The erasure of that data.

15. Employee Data

The rules and principles of Data Protection outlined in this Guide apply to our employees as they do to our

customers.

- Employees do not lose their privacy and data protection rights just because they are employees. We operate in an effective working environment which is balanced against our employees' reasonable expectation to privacy.
- Given the imbalance in power between employees and employers, consent cannot usually be given (or indeed withheld) freely, so other grounds for processing employee data must always be considered. Blanket monitoring of employees or their communications will be avoided. Any monitoring (or tracking) will be proportionate to the risks faced by us or the commercial benefits. The Policy on legitimate monitoring will be clear, transparent, and readily accessible. Private spaces (e.g. private mail or document folder) will be provided for employees.
- Blanket bans on communications/internet usage for personal reasons are disproportionate and impractical. Our communications/internet usage Policy is to allow staff to access the telephone for personal use when it is necessary in the event of an emergency at home or other tragic events. The internet is to be used for business use with the exception of internet banking if required.
- Job applicants will be informed before their social media profiles are reviewed and such pre-employment reviews will only take place where the particular job role warrants it.
- Similarly, in-employment screening of employees' social media profiles will not take place on a generalised basis. Employees will not be obliged to utilise an employer-provided social media profile.
- We will review our Speak Up procedures to ensure that whistle-blowers' confidentiality is safeguarded.
- Responses to employee Data Access Requests will respect the confidentiality of other employees or third parties.

16. Third Party Processors

Data is our most valuable asset, but also our greatest liability. In simple terms, we protect it if we need it and delete it according to statutory and non-statutory retention periods should it no longer be required or of no further value to our organisation.

We ensure that we validate the privacy notices of third-party processors respectively, to ensure that they are compliant with the requirements of GDPR.

17. Regulatory Powers & Sanctions

The DPC's Regulatory powers comprise investigative, corrective, authorisation and advisory powers and can be summarised as follows.

- To carry out Audits/inspections. See more on this below.
- To notify the firm of an alleged infringement.
- To request information.
- To have access to a firm's records.
- To have access to a firm's premises.
- To order the commission of a report by a "reviewer" which can be appointed by the DPC.

Corrective Powers & Sanctions

- To issue warnings to firms of possible infringements.
- To issue reprimands.
- To order a firm to comply with a data subject's request.
- To order a firm to comply with a certain requirement within a specified timeframe.
- To order a firm to notify a breach to a data subject.
- To order a limitation, restriction or ban on certain processing.
- To order rectification or erasure of certain personal data.
- To order the suspension of certain data transfers.
- To impose fines of up to €20m or 4% of the total worldwide turnover of the previous year. The following factors will be taken into account in determining any fine: -
- The nature, gravity, and duration of the breach, including the sensitivity of the data, the numbers of

data subjects affected and the impact on them.
- The intentional or negligent character of the breach.
- Any mitigating measures taken by the firm.
- The technical and organisational measures in place.
- Any previous breaches or history of non-compliance.
- The manner in which the DPC became aware of the breach.
- The extent to which the firm co-operated with the DPC.
- Adherence to any approved code of practice.
- To impose fines of up to €50,000 personally on Directors/Officers of the firm (but not the DPO).

Authorisation & Advisory Powers of ODPC
- Issuing opinions and approving draft codes of practice.
- To approve standard contractual clauses for use in processing contracts or for transfers of data outside the EU/EEA.
- To issue certifications and accredit certification bodies (e.g. for DPO certification courses).
- To bring legal proceedings against firms.
- Issuing annual reports including naming and shaming firms.

DPC Audits
- May be carried out at very short notice (even a matter of days in certain cases) requesting information in advance such as policies and documentation.
- May look at data processing carried out as a whole or specific aspects (e.g. following a complaint or infringement).
- Will usually adopt a questionnaire approach. Details of the standard questionnaire used along with self-assessment checklists are contained in the DPC's Guidance on Audits (below).
- Will be hands-on in terms of inspecting databases and records.
- Will involve interviewing the DPO, senior management and personnel involved in the relevant processing activities
- Full co-operation with the DPC is essential.

18. An individual's right to damages

Individuals will be able to claim damages for breaches of Data Protection in respect of their personal data even where no loss or damage has resulted. Individuals will be able to sue both our firm as Controller/Processor and any Processors our firm uses. A Not-for-Profit body can complain on an individual's behalf to both our firm and to the DPC and can take legal action on behalf of one or more individuals.

Appendix 1

Sample Data Access Request Form

[Name of Firm]
Customer Data Access Request Form

As our customer, you are entitled to request a copy of the personal data we hold about you within 30 calendar days and for no charge.
You are not obliged to use this form to request your data, but it helps us to process your request more promptly if you do.
Please provide the information requested in full using block capitals.
If there is something in particular you are looking for, please specify this.
You can post this form to us at the address above in which case we
will post your personal data to you. Alternatively, you can email this form to us at [email address] in which case we will send your personal data to the email address you provide us in a secure format.

1. Customer Name	
2. Postal Address	
3. Email Address ***(if you wish to receive your data by secure email)***	
4. Date of Birth	
5. Policy No.(s)	
6. If there is something in particular you are looking, please specify here giving as much detail as you can.	
6. Customer Signature	
7. Date	
Office Use Only Date Received	