BROKERS IRELAND
GENERAL DATA PROTECTION REGULATIONS

GDPR GUIDANCE

FEBRUARY 2018

Table of contents

Introduction

The Irish Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 ("the Acts") will shortly be (for the most part) replaced by a new Data Protection Act ("the Act") to give effect to EU legislation, known as the General Data Protection Regulation ("GDPR"), and will come into force on 25 May 2018.

While the current Data Protection Principles will remain, the Act will bring prescriptive new requirements and greater penalties for non-compliance which, Brokers need to be aware of as Data Controllers.

This guide aims to provide Brokers Ireland members with relevant information and practical guidance on the key provisions in a straightforward, easy to read format. It is based on the draft legislation and regulatory guidance available at 12 February 2018 and will be updated over time to reflect new developments.

The guide is provided for information purposes only and does not constitute legal advice. The legislation itself (see Section of this Guide) should always be considered the primary reference source. Members are also reminded to refer to the web site of the Data Protection Commissioner ("DPC"), dataprotection.ie, for updates. Click here for link (left click and Open Hyperlink).
https://www.dataprotection.ie/docs/Home/4.htm

Brokers Ireland
February, 2018

Section 1 – Data Protection Terms Explained

In this section, the most frequently used Data Protection terms are explained here in summary form and in Simple English; the Legislation should be referred to for the exact definitions (Refer to Section 16 of this Guide). Additional terms are explained in relevant Sections. Note: Terms which have changed by GDPR are marked in Red.

Automated Data means data held electronically or on computer.

Consent …of the data subject means a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by a statement or a clear affirmative action signifies agreement to the processing of personal data relating to him or her. **(Art. 4(11) GDPR)**

Data Subject means the individual about whom the personal data relates. For Brokers this means both your customers and staff.

Data Controller controls the data and its use. All Brokers are Data Controllers.

Data Processor processes the data on behalf of the Data Controller. Example payroll company.

Fair Processing
Fair processing has two distinct aspects and is not the same as having a legal basis for the processing:

- You must be transparent with individuals about what you're doing with their personal data and why.
- You must ensure you process personal information fairly. Broadly, this means you must process it in a way that individuals would reasonably expect.
- In addition to having a legal basis for processing personal data, you must process it fairly.

Manual Data means data held on paper or hard copy but only if it is part of a "relevant filing system".

Personal Data means data: **(S.63 DP Bill)**

- Relating to identifiable living individuals or
- Which could identify a living individual by reference to the data, such as by an identifier (e.g. name, identification number, location data, online identifier), or by reference to a specific factor(s) such as the physical, physiological, genetic, mental, economic, cultural, social identity of the individual.
- Includes criminal convictions and offences.
- Includes both automated and manual data.

Processing includes anything done on or to data, so therefore covers:

- Obtaining, recording or keeping data
- Collecting, organising, storing, altering or adapting data
- Retrieving, consulting or using data
- Disclosing data by transmitting, disseminating or making available
- Aligning, combining, blocking, erasing or destroying data.

Profiling means:
Any kind of automated processing which uses personal data to analyse or predict certain characteristics or preferences of an individual(s).

Relevant filing system means:

- Structured by reference to individuals (eg alphabetically by name);
- Organised in such a way that specific information relating to an individual is readily accessible;
- So if a file has an individual's name on the front, the content of that file is Personal Data. On the other hand, a file named "Miscellaneous" does not contain Personal Data.

Sensitive or Special Category Data means any personal data as to: **(S.2 DP Bill)**

(a) Racial or ethnic origin, or
(b) Political opinions or religious or philosophical beliefs, or
(c) Trade union membership, or
(d) Physical or mental health or condition or sexual life, or
(e) Biometric data; or
(f) Genetic data.

Note: Data relating to Criminal convictions and offences (including ongoing criminal proceedings) is no longer categorised as Sensitive data.

Section 2 – The 6 Data Protection Principles (S.65 DP Bill)

No changes to the Data Principles with GDPR

There are six basic rules of Data Protection referred to as the Data Protection Principles and, although their wording has changed slightly, their meaning stays the same post-GDPR. They are set out as follows along with relevant case studies from the DPC.

1. Process data (information) fairly.
Meaning:

- When collecting or recording data, you, the Broker, must be clearly identified and your address provided,
- Identify the purpose for collecting the data and to whom the data will be disclosed (insurers, others).
- This must be clear on application forms, notices must be displayed on CCTV where in use and where telephone calls are recorded callers must be advised.
- For more detail, see Section 5: The Grounds for Data Processing, and Section 6: Privacy Notices.

2. Collect data for one or more specified, explicit and legitimate purposes and use it only in ways which are compatible with those purposes.
Meaning:

- The data provided must only be used for the purposes as clearly stated to the customer.
- Customers must be given the option to consent to non-essential uses such as marketing or profiling for marketing purposes.
- For more detail, see Section 5: The Grounds for Data Processing, Section 6: Privacy Notices, Section 9: Direct Marketing.

3. Ensure that data is adequate, relevant and not excessive in relation to the purpose(s) for which it was collected.
Meaning:

- Customers should not be asked for information that's not needed for the stated purpose. There must be either a legal/regulatory requirement or a legitimate business need to hold data.
- Once collected, only the minimum data that's needed for a particular purpose should be used/disclosed (even internally in your firm) (known as "data minimisation").
- Note however: It may be the case that more information is collected for example on a Fact Find than is actually needed for the particular insurance products taken out or renewed at the time. Any excess data collected should not then be used for other purposes. However it makes sense to retain all that data for the next annual review so that the customer is not asked to provide the information again and at that stage the information can be updated if needs be.
- For more detail, see Section 5: The Grounds for Data Processing.

4. Keep data accurate and, where necessary, up-to-date and take all reasonable steps to erase or correct inaccurate data.
Meaning:

- Ensure that customers' data is updated promptly when notifications are received
- For more detail, see Section 5: The Grounds for Data Processing.

5. Retain data for no longer than is necessary for the specified purpose(s).
Meaning:

- You must be able to point to a particular requirement e.g. CPC, FSO etc. or a legitimate business need to retain data for a certain period. For example, as with the Fact Find example above (Principle 3), the Central Bank will require Fact Finds to be retained for a certain period for CPC purposes.
- Comprehensive Retention schedules must be held and actioned.
- Data must be destroyed securely e.g. by confidential shredding.
- Non- Personal Data, i.e. data which cannot identify a living individual, is outside the scope of this and the other Data Protection Principles.
- See Section 11: Data Retention.

6. Keep data safe and secure including taking appropriate technical or organisational measures against unauthorised access, alteration, disclosure, accidental loss or destruction of the data.
Meaning:

- What's appropriate will depend on the Broker's size and resources and the volume and sensitivity of the data held.
- For more detail, see Section 10: Data Breach Reporting & Security.

For DPC Case Studies, click here (left click and Open Hyperlink).
https://www.dataprotection.ie/docs/Case-Studies/945.htm

Section 3 – GDPR: A Summary of the Key Changes

The following are the key changes introduced by GDPR of relevance to Brokers. Further details on each are provided in this guide in the sections noted.

1. **Data Protection Officer (DPO)** – now mandatory if certain criteria are satisfied. (See Section 4: Data Protection Officer)

2. **Privacy Notices** – more information required, including the legal basis for processing and the retention periods or the rationale for them. (See Section 6: Privacy Notices)

3. **Health data** – new legal basis for processing customers' health data when providing insurance. (See Section 5: The Grounds for Processing)

4. **Criminal history data** - new legal basis for processing customers' criminal history when providing insurance. (See Section 5: The Grounds for Processing)

5. **Employee data** – new legal basis for processing employees' health or other sensitive/special category data. (See Section 5: The Grounds for Processing)

6. **Data access rights** – additional information to be provided, less time to provide data, must be able to provide data electronically if requested & no fee chargeable. (See Section 7: Data Subject Rights & Requests)

7. **Legal privilege** – has been broadened to cover all communications between a firm and its legal advisors regardless of whether legal proceedings or a claim is likely or anticipated. (See Section 7: Data Subject Rights & Requests)

8. **Data portability** – of certain customer data in a particular format both to the individual data subject and to another Broker now mandatory. (See Section 7: Data Subject Rights & Requests)

9. **Data security breach notifications** – now mandatory (already mandatory in practice in Ireland) & more breaches notifiable. (See Section 10: Data Breach Reporting & Security)

10. **Data Protection Impact Assessments ("DPIAs")** – now mandatory in certain circumstances. (See Section 12: Data Protection Impact Assessments)

11. **New Record of Processing Activities** – to replace the current ODPC Registration system. (See Section 13: Record of Processing Activities)

12. **New statutory right to damages** – now even in cases of non-material loss. (See Section 7: Data Subject Rights & Requests)

13. **New fining powers to Regulator** – up to €20m or 4% group annual turnover. (See Section 15: Regulatory Powers & Sanctions)

14. **New statutory obligations & criminal offences for Processors** – Processors and Controllers are now jointly liable for any data security breaches. (See Section 10: Data Breach Reporting & Security, and Section 15: Regulatory Powers & Sanctions)

Section 4 – Data Protection Officer (S. 82 DP Bill)

Do Brokers need to appoint a DPO?

- Not necessarily, but the legislation and current guidance is not definitive.
- What we know is that not all firms have to appoint a DPO.
- All controllers including Brokers must decide based on the criteria set out in the GDPR and the DP Bill (below) whether or not to appoint a DPO and Brokers Ireland would advise members to document the rationale for their decision.
- There is currently no exemption in the legislation or the Regulatory guidance for smaller firms or SMEs (such as the vast majority of Broker firms). The DP Bill does give the Minister power to issue regulations making such an exemption but no such regulations have been issued to date. The DP Bill does allow for the sharing of a DPO by two or more firms and there are no conditions for doing so.
- Brokers Ireland will update members on developments in this area.
- It's important to note that while Brokers Ireland will help with members' queries, Brokers Ireland is not a DPO for firms.

The Criteria (for firms in the private sector) for the requirement to appoint a DPO (shared or otherwise):-

1. **Large scale processing:** 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
2. **Sensitive/special category data:** Where the core activities of the organisation consist of special categories of data (ie health data) or personal data relating to criminal convictions or offences.

While the GDPR does not define large-scale the following factors should be taken into consideration:

- The number of individuals (data subjects) concerned – either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

Examples of large-scale processing provided by the ODPC include:
Processing of customer data in the regular course of business by an insurance company or a bank

Regular and systematic monitoring should be interpreted, in particular, as including all forms of tracking and profiling of individuals.

'Regular' is interpreted by the ODPC as meaning one or more of the following:

- Ongoing or occurring at particular intervals for a particular period

- Recurring or repeated at fixed times

'Systematic' is interpreted as meaning one or more of the following:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy

Examples of Regular & Systematic Monitoring provided by the ODPC include:
Profiling and scoring for purposes of risk assessment (eg fraud, credit scoring, insurance premiums).

For more detailed ODPC Guidance, click here (left click and Open Hyperlink).
http://gdprandyou.ie/data-protection-officer/

For more detailed EU Regulatory Guidance, click here (left click and Open Hyperlink).
http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

The criteria for a DPO:-

- May be a member of staff or an external contractor
- May be full-time or part-time
- May have other responsibilities in addition to Data Protection
- Must have "expert knowledge" of Data Protection and hold a professional certification. The DPC expects a greater degree of knowledge for those DPOs in certain sectors, including insurance. For more detailed Regulatory Guidance, click here (left Click and Open Hyperlink).

https://dataprotection.ie/viewdoc.asp?DocID=1643&ad=1

- Must be involved in all Data Protection matters and all new business initiatives involving personal data
- Must be given appropriate resources
- Must have appropriate independence – so for example, not the Principal of a one-person Broker firm.
- Cannot be dismissed or penalised for performing their Data Protection responsibilities
- Will not be personally liable for the firm's non-compliance with Data Protection
- DPO contact details must be published in a web site's Privacy Policy (a generic dpo email and postal address and will suffice).

Tasks of the DPO:-

- To inform and advise the organisation and its employees of their GDPR obligations
- To monitor compliance and to raise awareness/educate staff
- To carry out DPIAs
- To be the contact point with DPC

Section 5 – The Grounds for Data Processing

As well as processing the personal data of your customers and employees in accordance with the 6 Data Protection Principles (Section 2 of this Guide), your firm must also have a legal basis for processing each type of personal data you hold.

This section covers as follows:-

- The grounds for processing Personal (Non-Sensitive) Data
- The grounds for processing Sensitive Data
- The conditions for valid Consent
- Legitimate Interests as a legal basis
- Transfers outside of the EU/EEA

The grounds or Legal Basis for Processing – Personal Data (including Criminal History data) (Art 6(1) GDPR & S.49 DP Bill)

One of the following grounds must be satisfied in order to process Personal Data:-

1. **Consent -** Consent of the data subject (See below for conditions for valid consent);
2. **Contract -** Necessary for the performance of the contract (or in the case of Brokers to provide the insurance product);
3. **Legal Obligation -** Necessary to comply with a legal obligation;
4. **Vital Interests -** Necessary to protect the vital interests of the data subject;
5. **Public Interest -** Necessary for the performance of a task in the public interest or in the exercise of an official authority – included for completeness but not applicable to Brokers; or
6. **Legitimate Interests -** Necessary for the legitimate interests of the data controller, unless such interests are overridden by the interests of the data subject (See requirements below); and
7. **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.

Legal Bases for Processing – Sensitive/Special Category Data (eg Health data):- (Art 7 GDPR & S.39 - 44 DP Bill)

One of the following grounds must be satisfied in order to process Sensitive Data:-

1. **Explicit Consent –** Explicit consent of the data subject (See below for conditions for valid consent);
2. **Vital Interests -** Necessary to protect the vital interests of the data subject where the data subject is incapable of giving consent;
3. **Insurance and Pension purposes** – Necessary and proportionate for the purposes of providing an insurance, pension or mortgage product;
4. **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;

5. **Medical Assessment/Diagnosis/Treatment –** Necessary for the purposes of preventative/occupational medicine, the assessment of the working capacity of an employee, medical diagnosis;
6. **Legal Advice and Legal Proceedings –** Necessary for obtaining legal advice whether or not in the context of a claim (or prospective claim);

The following grounds are either not applicable or unlikely to be applicable to Brokers but included here for completeness:

7. **Substantial Public Interest –** Necessary for reasons of substantial public interest (no Regulatory guidance yet);
8. **Public Interest in the area of Public Health -** (GDPR specifies that this is not a ground open to insurance companies);
9. **Archiving, Research or Statistical –** Necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (not likely to be applicable to Brokers);
10. **Not For Profit bodies –** Processing in the course of their legitimate activities (not applicable to Brokers);
11. **Data made public –** by the data subject (not likely to be applicable to Brokers).

Consent & Explicit Consent – the conditions for a valid consent are:- (Art.7 GDPR)

- There is no practical difference between "Consent" and "Explicit Consent". Both require as follows:
- **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 -** Must 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 -** Must be specific to the particular options given, so for example a customer must be able, should they wish to, to withhold their consent to Profiling for Marketing purposes but to consent to Marketing itself. So if consent is requested in the form of a written declaration, then the different options must be set out individually and separate consents requested for each option, and in an intelligible easily accessible format using clear and plain language.
- **Recorded -** Must be verifiable, a record must be kept of how and when consent was given. So, consent can be confirmed over the phone but then recorded thereafter and this should be proceduralised.
- **Can be withdrawn at any time.**
    - It must be made easy for consent to be withdrawn.
    - Prior to giving consent, a data subject must be informed of their right to withdraw their consent at any time.
- **NB: The new requirements for Consent do not change existing Marketing rules (See Section 9: Direct Marketing).**

Regulatory guidance on Consent is awaited.

Legitimate Interests as a legal basis: (Art .6(1) GDPR)

Legitimate Interests may be an appropriate ground when your firm wishes 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, a firm must:-

1. **Be transparent**: Inform data subjects in your firm's Privacy Policy of both the processing and the Legitimate Interests for it plus their right to object (on "compelling legitimate grounds" only); and
2. **Carry out an assessment** and document your rationale, including the safeguards in place for data subjects. When doing so, consider the actual effect of the processing on individuals, ie rather than an academic or abstract exercise; and
3. **Keep documentation** available for inspection by the DPC.

The Legitimate Interests Assessment must include the following:-

1. **The rationale for relying on Legitimate Interests** and why the other grounds are not appropriate;
2. **A description of your firm's particular Legitimate Interests** (e.g. the commercial benefits) and the factors that make these Interests (i) Lawful; (ii) Concrete; and (iii) Real and tangible ie not speculative;
3. **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;
4. **A provisional assessment** as to whether your firm's Interests are overridden by the rights of the data subject(s), taking into account:
    a. The possible prejudice if the proposed processing does not go ahead (or continue);
    b. The nature of the data involved;
    c. The status of the data subject(s) relative to that of your firm (is it unequal?);
    d. The way the data is processed and the impact on the data subject(s);
    e. The data subject's reasonable expectations;
    f. The impact versus the benefits of the processing; and
    g. While not required: The benefits if any to the data subject(s).
5. **A final assessment** taking account of additional safeguards, such as:
    a. Data minimisation: e.g. strict limitations on the data collected, immediate deletion of data after use;
    b. 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");

c. Use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, DPIAs;
d. Increased transparency, right to opt out, data access and data portability rights available to the data subject(s).

For more detailed Regulatory Guidance on Legitimate Interests, click here (left click and Open Hyperlink).
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Transfers outside the EU/EEA: Some changes with GDPR but largely the same rules apply:- (S.91-95 DP Bill)

- Firms cannot transfer personal data outside the EU/EEA unless certain conditions (or grounds for processing) are satisfied.
- "Transfers of data" include:
  - Sharing personal data with other companies within the same Group;
  - Enabling access by third parties located outside the EU/EEA to personal data on your systems here in Ireland; &
  - Storing your personal data on the Cloud if the Cloud facility is located outside the EU/EEA.
- Further detail on Transfers outside the EU/EEA is outside the scope of this Guide. Legal advice should always be sought.

Section 6 – Privacy Notices (Art.13, 14 GDPR)

Privacy Notices must contain the following information:

- In "a concise, transparent, intelligible and easily accessible form, using clear and plain language".
- The words in underlined italics indicate the new requirements under GDPR:-

1. The firm's name and contact details;
2. *The DPO's contact details;*
3. The different types and categories of personal data held;
4. The purpose of the processing and *the legal basis for the processing;*
5. *Where this ground is relied upon: The firm's legitimate interests and an explanation of those interests;*
6. The recipients or categories of recipients to whom data is shared/disclosed;
7. *Details of any transfers outside the EEA, the safeguards in place and the means by which to obtain a copy of them;*
8. *The data retention period or the criteria used to determine the data retention period;*
9. The individual's rights including: the right of access to data, rectification *and erasure, restriction of processing, objection to processing, data portability;*
10. *Where the processing is based on Consent, the right to withdraw consent at any time;*
11. *The right to complain to the DPC;*
12. Details of any automated decision-making including profiling and the logic involved as well as the significance and consequence for the individual;
13. *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;*
14. **And in addition as expected by the DPC:** The security of the data collected should be mentioned and in general terms the measures taken to ensure the security of data.

https://www.dataprotection.ie/docs/EN/24-10-2017-International-data-protection-authorities-enforcement-operation-finds-website-privacy-notices-are-too-vague-and-generally-inadequate/m/1674.htm

Suggested action points

- Review your firm's Privacy Policy.
- Add the additional information required.
- Consider the length of the notice and whether a "layered" notice would be easier to follow, eg a short notice with links to more detailed information.
- Consider whether the language and terminology used is clear and easy to understand.
- For firms which receive data from corporate bodies or trusts (and so rely on them to obtain consents), make sure there is a legal agreement in place.
- For examples of good and bad Privacy Notices in practice, click here (left click and Open Hyperlink).

https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf

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

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

1. Right of Access (S.86 DP Bill)

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 your firm.
- Template Request forms are useful but cannot be 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.
- For a sample Data Access Request Form, refer to Appendix 2 of this Guide.

Charging for Requests:-

- A fee may not be charged, however small.
- However, in very exceptional circumstances, a firm is entitled to charge a fee to cover administrative costs if it reasonably believes that the request will take more than 90 calendar days to respond to and will involve considerable effort and resources. It would be advisable to inform the data subject as soon as possible that this is the case and in any case to provide them with as much data as can be provided in the meantime. (See "Disproportionate Effort" below.)

Timeframe for responding:-

- 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: must inform the individual of the need for the extended period and must provide as much of the data as possible in the meantime.
- Firms can decide on their own criteria for proving identity and should document this as part of their procedures. For example, it would be safe to assume that a request received from a person's known address is proof of their identity, but some firms may insist on additional details such as date of birth. In addition, signatures can usually be presumed to be correct.

Format of Response:-

- Must include a copy of the data in an intelligible form i.e. photocopies must be legible, abbreviations only understood by your firm must be explained.
- Must be provided by email if the request is received by email, unless otherwise requested.
- Must inform the individual if no information is held about them.
- Must 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 very limited grounds for restricting or refusing a data subject access request. The grounds available are:-

(i) **Legal Privilege.**
This ground has been broadened by GDPR and covers all communications between the firm (the data controller) and their legal advisors (internal/external) regardless of whether legal action is likely or anticipated.

(ii) **Third Party data.**
References identifying other (third) parties, for example the names of other customers, must be removed (redacted). However, references to staff who would be known to the customer (eg the staff member who the customer has dealt with) should be retained.

(iii) **Opinions given in Confidence.**

References to third parties (e.g. Individuals in previous employers) who have given Employment References in confidence must be redacted.
Similarly references to the identity of whistle-blowers or witnesses in an internal investigation must be redacted, unless consent has been given.
It is not enough that a document has been headed "Confidential"; as a firm you must be able to demonstrate that the document was given with the expectation that it would not be disclosed to the particular individual.

(iv) **Ongoing Criminal or internal misconduct investigation.**

Data can and should be withheld where there is an ongoing Gardai investigation concerning the individual (eg 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.

(v) **Commercially sensitive data.**

Any data which would be commercially damaging or disadvantageous if known to a firm's competitors or customers can be removed.
Example: References in internal meeting minutes to a Broker firm's pricing policy.

(vi) **Health data where harmful.**

Health data can and must 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 must not of course be mentioned.
Please click link for further information - https://www.dataprotection.ie/docs/Data-Protection-Access-Requests-for-Personnel-Records/m/206.htm

(vii) **Disproportionate effort.**

Where a firm 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 should 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:
(i) 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 period.
(ii) Inform the individual if the firm chooses to charge an admin fee.
(iii) Document internally the particular circumstances of the Request to evidence the rationale for relying on this ground.

(viii) Repeat requests.

A firm is entitled to refuse to respond to repeated requests within particular 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.
Best practice: Decide on a policy for your firm and document it in your procedures. 12 months is considered by the DPC a reasonable minimum interval between requests.

(ix) Repeat requests which are "manifestly unfounded or excessive in particular because of their repetitive character".

Can be refused.

(x) 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 eg by advisors. The following practice is recommended:-

- 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.
- 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 doesn't affect dealing with operational requests in the usual way.
- Public representatives. Must 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. 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. Best practice to 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 be disclosed by the NVDF (the National Vehicle Driver File).

For DPC Case Studies, click here (left click and Open Hyperlink).
https://www.dataprotection.ie/docs/Case-Studies/945.htm

2. Right of Data Portability (Art.20 GDPR)

This is a new right, the customer's right to receive their data, not in hard copy or by email like a subject access request but, in 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 as follows:-

Only the following data is covered

- The data provided to the firm by the individual themselves.
- And any observed data (eg 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 (arguably all staff data bar internal recruitment, succession planning data but consider each request on a case by case basis).
- Excludes data produced by subsequent analysis of data provided by the individual, ie inferred or derived data (eg risk scores).

Format

- Not prescribed but must be secure and must allow the data to be used and re-used (ie, in an interoperable, machine-readable format)
- Regulatory guidance suggests the following for direct transmission of data: The use of industry-standard formats already in use or, where none in use, commonly used open formats eg XML, JSON, CSV.
- In cases of large amounts of data, Regulatory guidance suggests the following for the retrieval of data: Secure messaging, an SFTB server, secured WebAPI or WebPortal.
- The agreement of industry-wide solutions is encouraged.

Fee

- Not chargeable (unless it can be demonstrated that the request is unfounded or excessive or the requests too frequent – very unlikely given the API (Application Programming Interfaces) technology available).

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.

For more detailed Regulatory Guidance, click here (left click and Open Hyperlink).
http://ec.europa.eu/newsroom/document.cfm?doc_id=44099

DPC Case Studies on Portability are expected post-GDPR (May 2018).

3. Right of Rectification (S.87 DP Bill)

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

4. Right to have processing restricted or stopped (S.87 DP Bill)

Individuals may request a firm to stop their data being used for certain purposes eg, for direct marketing. This is in effect the equivalent of an Opt Out request and must be recorded as such on the firm's system.

5. Right of Erasure & Right to be Forgotten (S.87 DP Bill)

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 your Retention Schedule**. It is important therefore that firms document their Retention Schedules and action them accordingly. Most queries/requests for erasure can then be easily answered with reference to your firm's retention policy.

Similar to the right to Erasure is the new right To Be Forgotten under GDPR, however the right to be forgotten (or to be de-listed) **does not apply to the financial services sector and is included here for reference only.**

6. Right to Complain to the DPC (S.114 DP Bill)

- This is described in more detail in Section 15 (Regulatory Powers & Sanctions).
- Note: A 'Not For Profit' agency can complain on an individual's behalf to both your firm and to the DPC and can take legal action on behalf of one or more individuals.

7. Right to Sue the Controller and Processor (S.112 DP Bill)

- New statutory right to damages – now even in cases of non-material loss.
- Individuals will now be able to claim damages for breaches of Data Protection in respect of their personal data – even where no loss or damage has resulted.
- Firms are advised to take extra care in particular when responding to Access and other requests from individuals, to ensure that the risk of any such claims is minimised.
- Individuals will be able to sue both your firm as Controller and any Processors your firm uses. Firms are advised to review all contracts with Processors to ensure the adequacy of Processors' Data Protection obligations.
- A Not For Profit body can complain on an individual's behalf to both your firm and to the DPC and can take legal action on behalf of one or more individuals.

Section 8 – Automated Decision-Making & Profiling (S.51, 84 DP Bill)

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. There are different rules for each and, for both, new requirements under GDPR. This section focuses solely on the relevant aspects for Brokers.

Automated Decision-Making

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").

Example – The giving of quotes and indicative quotes on-line

The individual (customer in this case) when looking for a quote or an indicative quote on-line has the right to the following:-

(i) To be informed that an Automated Decision-Making process is involved;
(ii) To be informed that the quote is generated using the data provided by that individual and applied to an internal logic or set of criteria;
(iii) To be informed in general terms of how that internal logic or set of criteria determines the quote, so for example the more penalty points on the individual's driving licence the higher the premium quoted for motor insurance; and
(iv) Following the quote, the right to have that quote reviewed by a sufficiently senior member of staff.

GDPR – Guidance

If your firm carries out Automated Decision-Making, you must ensure that:-

(i) The required information is clearly provided on the particular section of your web site; and
(ii) Your firm has a documented process for the review of decisions and queries from individuals.

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, behaviour, 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).

Examples

- **Profiling for Marketing purposes – e.g., to identify which of your firm's motor insurance customers are most likely to want home insurance.**
- **Risk assessments for fraud prevention/AML purposes.**

The requirements

In all cases of Profiling, the individual has the right to the following:-

(i) To be informed that they will be subject to Profiling; and
(ii) An explanation of the meaning of Profiling and the purpose for which it is being carried out.
(iii) Accordingly, all instances of Profiling and the purpose of each must be described in your firm's Use of Information Notice and on application forms.

In certain cases (only), the individual also has the right to Object/Opt Out of such Profiling. These are where the Profiling is:-

(i) Not required for the performance of the contract (i.e. to provide the insurance product); OR
(ii) Not required for any legal or regulatory reasons.

So, in the above examples:-

- Your firm's application form must contain an Opt Out from Profiling for Marketing purposes but not for Fraud Prevention or AML.
- This Opt Out is best located directly following the section on Marketing preferences.
- The Opt Out from Profiling must be recorded separately on your system – this will require a systems change.

For more detailed Regulatory Guidance on Automated Decision-Making and Portability, click here (left click and Open Hyperlink).
http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963

Data Protection Impact Assessments

From May 2018, all new Profiling or Automated Decision-Making initiatives will require a Data Protection Impact Assessment ("DPIA") to be carried out in advance (See Section 12 of this Guide).

Section 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.

No changes to the rules with GDPR

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 be Opt Ins. This is not the case. GDPR makes no changes to the current Marketing rules. GDPR does however recognise Marketing as a Legitimate business activity. **(Recital 47 GDPR)**

Note: At time of writing, new ePrivacy Regulations are expected in 2018 however it is too early to predict with any certainty how Marketing rules with respect to Email will be impacted.

Basic rule

The basic rule that applies to direct marketing is that the data controller needs the consent of the individual to use their personal data for direct marketing purposes. The marketer must make his/her identity clear and disclose how the individual's contact details were obtained.

Different rules apply depending on the format used for the marketing. These are as follows:-

Post

- You must tell your customers (or potential customers) that you 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, by providing a "tick-box" on an application form).
- An individual may withdraw consent to direct marketing at any time. The data controller has 28 days to comply with a request to cease direct marketing.
- For non-customers, you 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.

To access the Edited Electoral Register, click here (left click and Open Hyperlink).
http://www.checktheregister.ie/PublicPages/Default.aspx?uiLang=

Telephone

- You must tell your customers (or potential customers) that you 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, by providing a "tick-box" on an application form).
- In the case of a **customer,** you can call them even if they have opted out from receiving marketing calls on the National Directory Database ("NDD"), i.e. the consent given to your firm outweighs the preferences recorded on the NDD and so you do not need to check the NDD.
- However in the case of a **non-customer**, you must check the NDD for any opt outs recorded before calling that individual, i.e. the NDD opt out will override any consent given to your firm.

To access the National Directory Database, click here (left click and Open Hyperlink).
http://www.openeir.ie/NDD/

SMS Messages

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

EMail – individuals and business customers

- At the point of sale, you must tell your customers that you 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, by providing a "tick-box" on an application form).
- For those customers who do not Opt Out, you can email them for marketing purposes, so long as:-
    (i) Its within 12 months of the initial point of sale and receipt of their email details;
    (ii) The product or service being marketed is your own;
    (iii) 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);
    (iv) In the email (and all subsequent emails), the customer is given a clear opt-out not to receive further such emails;
    (v) 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**: You must 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) - you can email them for marketing purposes as long as their business or official email is received by you in the context of commercial or official activity or is listed in a Business Directory.

GDPR – Suggested Action Points

- Confirm your customers' marketing preferences at your next telephone or online interaction with them, eg at their next renewal, and at least annually going forward. Make sure this is documented in procedures.
- GDPR does not require that you write out or contact all your customers to confirm their marketing preferences.
- An individual may update their marketing preferences or withdraw consent to direct marketing at any time. Make sure:-

(i) There is a clear and simple contact point available to individuals (eg a dedicated email address provided as part of the Use of Information Notice on an application form and on your firm's web site);
(ii) If the request is received by letter, you must not insist the individual uses the dedicated email address instead;
(iii) There is clear process in place in your firm to action such requests and update your system promptly (at the very latest within 28 days of receiving the request).

Buying in Marketing Lists

- You can continue to buy leads lists from marketing companies, but best to confirm that their consents are explicit enough before 25 May 2018 by checking them first against your own system for any preferences indicated to your firm and then against the National Directory Database (for phone) and Electoral Register (for post).
- More generally:-
    - Only use reliable marketing firms; do your research and check for customer complaints;
    - Have a contract in place with the marketing firm which requires them to be DP and GDPR compliant;
    - When marketing to the leads on the list, refer to the name of the marketing firm as your source for their contact details.

Record Retention

- Failure to comply with the rules can attract heavy penalties (currently up to €5,000 per individual marketing contact).
- The onus is on you the Data Controller to prove that you had the required consent to send the marketing message.
- The record must be sufficiently granular to confirm the individual's name, the date they gave or altered their consent and the means by which they did so, ie email/letter/phone.
- Best practice: Retain such consents for a period of two years after the sending of the most recent marketing message to the recipient.

For DPC Guidance & Case Studies, click here (left click and Open Hyperlink).
https://www.dataprotection.ie/docs/DIRECT-MARKETING-A-GENERAL-GUIDE-FOR-DATA-CONTROLLERS/905.htm
https://www.dataprotection.ie/docs/Case-Studies/945.htm

Section 10 – Data Breach Reporting & Security

In the first section we look at what to do in the event of a personal data breach and in the second, what measures are expected to be taken in relation to the security of data.

Data Breach Reporting (S.79, 80, 81 DP Bill)

A Personal Data Breach is:-

- A breach of security
- Resulting in the accidental or unlawful
- Destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

A Data Breach is reportable to the DPC:-

- 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.
    - Accordingly, more breaches are likely to be reportable post-GDPR.
- In the meantime, all reasonable efforts must be made 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 (ie 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 has been contained.
- Unencrypted lap top: One of the firm's lap tops containing customer data is mislaid and is not encrypted, that breach must be reported to the DPC.

Format & content of report to DPC:-

- The report must be emailed to dpcbreaches@dataprotection.ie
- The content of the report is prescribed and must contain the following:-

(i) A description of the records involved including the type and category of the data;
(ii) The numbers of data subjects affected;
(iii) The likely consequences of the breach;
(iv) The measures taken or planned to be taken to recover/secure the data; and
(v) The contact details of the firm's DPO or other contact point in relation to the breach.

(vi) In addition, while not a requirement, it's good practice to include: The cause of the breach (e.g., human error or systems error).

- Best practice: Where a firm is required to report breaches to the DPC regularly eg on a weekly basis, it's preferable to report several at a time in a single email rather than individually.
- For a sample Data Breach Report template, refer to Appendix 3 of this Guide.

A Data Breach is <u>also</u> notifiable to the data subject(s):-

- Without undue delay once becoming aware of the breach (unless on the rare occasion investigating authorities request a delay);
- <u>You do not have to notify the data subject in all cases;</u>
- Only where there is a <u>high risk</u> to the rights of the data subject(s), ie
    - Where the security of the data has been compromised; and
    - The data is sufficiently sensitive or financial in nature so as 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 a public communication would be more appropriate.

Practical examples:

- <u>Mailing label error (above):</u> Where the customer correspondence contains sensitive data, eg health details, and is opened by the third party recipient, then assuming the customer is not already aware, they must be informed.
- <u>Unencrypted lap top (above):</u> Where the lap top contained customers' bank details and there's a risk to the security of the customers' accounts, then the customers must be informed.

Format & content of notification to the data subject(s):-

- No particular format.
- The notification must contain the following:-

(i) A description of the nature of the breach;
(ii) The name and contact details of the firm's DPO or other contact point in relation to the breach;
(iii) 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 it's adverse effects; and
(v) The specific advice to the data subject(s) to protect their data (e.g. resetting passwords where access credentials have been compromised).

Note: The criteria above for reporting to both the ODPC and to the data subject(s) replace those in the DPC's Code of Practice on Data Security Breach Reporting.

For more detailed Regulatory Guidance, click here (left click and Open Hyperlink).
http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47741

A Data Breach is also Reportable to the Central Bank:-

- Where there's a Cyber Security element to the breach, e.g. a hacking in to your firm's systems,
- Which could have a significant and adverse effect on your firm's ability to provide adequate services to your customers.

For detailed CBI Guidance on Cyber Security Incidents, link here (left click and Open Hyperlink).
https://centralbank.ie/docs/default-source/Regulation/how-we-regulate/policy/cross-industry-guidance-information-technology-cybersecurity-risks.pdf?sfvrsn=2%20

Incident Response Plan

- Make sure your firm has an Incident Response Plan in place detailing exactly who does what and when.
- Make sure it's reviewed for GDPR.

Record-keeping

- A record must 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 your firm's behalf by a Processor, there must be a written contract in place.
- The legislation requires that such a contract specifies (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 your firm's 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.
- Processors are now obliged by statute to immediately notify your firm of breaches.
- Processors are now jointly liable with Controllers for data security breaches. The DPC can attribute liability to both your firm and your Processor(s) and levy fines on both.

Data Security obligations (S.32, 65, 66, 71, 72 DP Bill)

Data controllers must implement:-

- "Appropriate technical and organisational measures"
- To ensure that the level of security is appropriate to the risks presented by both the nature of the personal data held and the particular processing activities.
- Must be able to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems.
- Must be able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- Must allow for the regular testing of security measures.
- Cost is no longer a factor.
- So a higher standard is required under GDPR.
- But it does not need to be "state of the art" technology.
- Compliance with approved codes of conduct, industry standards or certifications can be relied on to demonstrate compliance.
- The data controller must ensure that all employees and contractors are aware of these measures and comply with them.
- All contracts with data processors must oblige them to have GDPR-compliant security measures in place and to guarantee GDPR-compliant security standards.

Technical measures will usually 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)

Organisational measures will usually include:-

- Clear documented security policies communicated regularly to all employees and contractors.
- Security of premises (alarms/locks/lighting).

- Securing/locking away of 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.
- Securing/locking away of laptops and other portable equipment and computer media like discs or memory sticks locked securely at night.
- Confidential disposal of paper waste containing personal information, eg by shredding.

For DPC Case Studies, click here (left click and Open Hyperlink).
https://www.dataprotection.ie/docs/Case-Studies/945.htm

Section 11 – Data Retention

ONE OF THE BASIC PRINCIPLES
A FUNDAMENTAL REQUIREMENT IN A BROKER'S BUSINESS

The basic rules (S.65 DP Bill)

- Personal data may only be held for as long as necessary, i.e.
  (i) For as long as required under legal or regulatory requirements; or
  (ii) For as long as required for legitimate business purposes.
- By way of examples:-
  (i) FSO requirements on long term investment products or mortgages;
  (ii) Restrictions on retaining data on Spent convictions (the "7 year rule"); and
  (iii) CBI/CPC requirements on retaining Fact Finds.
- Data should never be kept on a "just in case" basis.
- Documented Retention Schedules setting out the retention periods and their rationale for each category of data must be in place.
- Retention Schedules must be reviewed periodically (best practice: annually) to ensure their completeness.
- Data must be purged/deleted in line with the Retention Schedules and clear responsibility for doing so assigned within the firm.
- Firms must ensure that all paper files, including those kept in archive or off-site storage, are destroyed securely.

For a sample Retention Schedule format, refer to Appendix 4 of this Guide.

For DPC Case Studies, click here (left click and Open Hyperlink).
https://www.dataprotection.ie/docs/Case-Studies/945.htm

Section 12 – Data Protection Impact Assessments ("DPIAs")
S.78 DP Bill

Data Protection Impact Assessments (also known as Data Privacy Impact Assessments or Privacy impact Assessments) are assessments carried out by firms 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.

When must DPIAs be carried out?

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

1. 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 upgraded; or
2. Automated decision-making or profiling is involved, e.g. risk scoring or quoting premiums on an automated basis; or
3. Systematically monitoring of your employees' activities (e.g. email, internet usage); or
4. Processing sensitive personal data on a large scale - e.g. health data or data relating to criminal history; or
5. Systematic monitoring of publicly available area(s), e.g. CCTV; or
6. Sharing or transfers of personal data outside the EU/EEA even between different companies within the same Group.

Form and content of a DPIA

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

1. A detailed description of the processing;
2. A simple data flow diagram which would be understood by the end customer/lay-man (comprising data sources, data processes/uses and data disclosures);
3. Reference to complying with any approved Industry Code of Conduct (eg the Code of Conduct for Data Protection in the Insurance Sector);
4. An assessment of the necessity and proportionality of the processing (including any alternatives considered);
5. A description of the Data Protection risks and the extent to which they will be managed, ie the controls/mitigants and actions required (if any) for each;
6. The extent to which interested parties were consulted (eg the DPO, internal stakeholders giving names and job titles, external parties such as suppliers/processors);
7. An overall assessment of the Residual Risk to data subjects (customers, employees);
8. This should be signed, dated and a copy saved to pdf format for an audit trail;
9. 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.
10. DPIAs must be made available to the DPC on request.

For a sample DPIA format, link here and go to Annex Two on page 34.
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

For more detailed Regulatory Guidance, link here.
http://gdprandyou.ie/data-protection-impact-assessments-dpia/

http://ec.europa.eu/newsroom/just/document.cfm?doc_id=44137

Section 13 – Record of Processing Activities

There are two new Records required:-

1. A Record of Processing Activities (S.75 DP Bill)

- 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 must contain the following details:-

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

For a sample Record format, refer to Appendix 4 of this Guide.

2 A Data Log of Automated Processing Systems (S.76 DP Bill)

The Log must contain the following details:-

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

Guidance is not yet available on the format or exact content of such a Log.

Section 14 – Employee Data

The rules and principles of Data Protection outlined in this Guide apply to a firm's employees as they do to a firm's customers.

There are however additional aspects for a firm (as both data controller and employer) to consider which are unique to employee data and particular challenges when processing personal data in a workplace environment, and this is increasingly the case given the latest developments in technology and changes in the way work takes place.

Guidance

1. Employees do not lose their privacy and data protection rights just because they are employees. Your firm's right to operate an effective working environment must be balanced against your employees' reasonable expectation to privacy.
2. 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. The DP Bill now gives a legal basis for processing employees' health or other sensitive/special category data. (**S.40 DP Bill** See Section 5: The Grounds for Processing).
3. Blanket monitoring of employees or their communications should be avoided. Any monitoring (or tracking) must be proportionate to the risks faced by the employer or the commercial benefits. The Policy on legitimate monitoring must be clear, transparent and readily accessible. Private spaces (e.g. private mail or document folder) must be provided to employees.
4. Blanket bans on communications/internet usage for personal reasons are disproportionate and impractical. The Usage Policy must be clear about what is and is not allowed.
5. When considering the deployment of new technologies, employers must minimise the amount and extent of personal data used or retained. Best practice: Consult your employees beforehand.
6. Job applicants must be informed before their social media profiles are reviewed and such pre-employment reviews must only take place where the particular job role warrants it.
7. Similarly, in-employment screening of employees' social media profiles should not take place on a generalised basis. Nor should employees be obliged to utilise an employer-provided social media profile.
8. Review your firm's Speak Up procedures to ensure that whistle-blowers' confidentiality is safeguarded.
9. Responses to employee Data Access Requests must respect the confidentiality of other employees or third parties.

For more detailed Regulatory Guidance, link here (left Click and Open Hyperlink).
http://ec.europa.eu/newsroom/document.cfm?doc_id=45631

Section 15 – Regulatory Powers & Sanctions

The DPC's Regulatory Powers (S.124-136 DP Bill)

The DPC's Regulatory powers comprise investigative, corrective, authorisation and advisory powers and can be summarised as follows. They are equally applicable to Controllers and Processors.

Investigative Powers

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

Corrective Powers & Sanctions

1. To issue warnings to firms of possible infringements.
2. To issue reprimands.
3. To order a firm to comply with a data subject's request.
4. To order a firm to comply with a certain requirement within a specified timeframe.
5. To order a firm to notify a breach to a data subject.
6. To order a limitation, restriction or ban on certain processing.
7. To order rectification or erasure of certain personal data.
8. To order the suspension of certain data transfers.
9. 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:-
    a) 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;
    b) The intentional or negligent character of the breach;
    c) Any mitigating measures taken by the firm;
    d) The technical and organisational measures in place;
    e) Any previous breaches or history of non-compliance;
    f) The manner in which the DPC became aware of the breach;
    g) The extent to which the firm co-operated with the DPC;
    h) Adherence to any approved code of practice.
10. To impose fines of up to €50,000 personally on Directors/Officers of the firm (but not the DPO).

Authorisation & Advisory Powers

1. To issue opinions and approve draft codes of practice.
2. To approve standard contractual clauses for use in processing contracts or for transfers of data outside the EU/EEA.
3. To issue certifications and accredit certification bodies (eg for DPO certification courses).
4. To bring legal proceedings against firms.
5. To issue 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 (eg 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.

For more detailed Regulatory Guidance on DPC Audits, link here (left click and Open Hyperlink).
https://www.dataprotection.ie/docimages/documents/GuidetoAuditProcessAug2014.pdf

An individual's right to damages (S.112 DP Bill)

- Individuals will now be able to claim damages for breaches of Data Protection in respect of their personal data – even where no loss or damage has resulted.
- Firms are advised to take extra care in particular when responding to Access and other requests from individuals, to ensure that the risk of any such claims is minimised.
- Individuals will be able to sue both your firm as Controller and any Processors your firm uses. Firms are advised to review all contracts with Processors to ensure the adequacy of Processors' Data Protection obligations.
- A Not For Profit body can complain on an individual's behalf to both your firm and to the DPC and can take legal action on behalf of one or more individuals.

Section 16 – The Legislation

For the Data Protection Bill 2018, click here (left click and Open Hyperlink).
http://www.oireachtas.ie/documents/bills28/bills/2018/1018/b1018s.pdf

For GDPR, click here (left click and Open Hyperlink).
http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

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 (encrypted) format.	
1. Customer Name *(Please give us your full name)*	
2. Postal Address *(Please give us your correspondence* 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**	

Appendix 2
Sample Data Security Breach Report Form

Data Security Breach Report Form	
[Name of Firm] **[Contact details]**	
Date of Report: [ ]	
• This report must be emailed to dpcbreaches@dataprotection.ie within 72 hours of the firm becoming aware of the data security breach.	
1. Date the breach occurred	
2. Date the firm became aware of the breach	
3. Types and categories of person data involved **(*indicate whether any sensitive data eg health data was involved)***	
4. The number of data subjects affected	
5. A description of the nature of the breach	
6. The likely consequences of the breach for the data subject(s)	

7. Whether the data subject(s) has been informed and if not give the reasons for not doing so	
8. The cause of the breach	
8. The measures taken to safeguard the data or mitigate the effects of the breach	
9. The measures taken to recover the data	
10. What further measures are planned to be taken if any	
11. Any other relevant information	

Appendix 3
Sample Retention Schedule Format

Data Retention Schedule							
A. Customer Data							
Ref. no.	**Record type**	**Manual or Auto**	**Location held**	**Purpose held**	**Retention period**	**Rationale**	**Comments**
B. Employee Data							
Ref. no.	**Record type**	**Manual or Auto**	**Location held**	**Purpose held**	**Retention period**	**Rationale**	**Comments**

Appendix 4
Sample Record of Processing Activities Format

Record of Data Processing Activities	
1. The Broker's name & address	
2. DPO's name & contact details	
3. Categories of personal data held	
4. Categories of data subjects	
5. Categories of persons or third parties to whom personal data disclosed (incl. other companies with the same Group)	
6. The type of processing carried out and the purpose(s) of each	
7. Retention periods for each category of personal data (or reference to a detailed Retention Schedule)	
8. Any transfers of data outside the EEA and the safeguards in place	
9. The technical and organisational security measures in place (with reference to the firm's Security Policy(ies) (naming them specifically.	

Aide-memoire for members:-

- Word documents
- CRM Systems e.g. Applied, Money advice & Platforms
- Email, Outlook, Office 365
- Storage discs, Laptops Phones USB Keys etc.

Supplementary Brokers Ireland Templates

Privacy Notice Template

ABC Ltd is committed to respecting and protecting your privacy and would like you to feel safe when you give us your personal details. We will always clearly identify ourselves in correspondence and on our website. Our principal business is to provide advice and arrange transactions on behalf of clients in relation to life & pensions/mortgages/general insurance products.(Please amend as appropriate)
To provide you with relevant information, respond to your requests we sometimes request that you provide us with information about yourself.
This Privacy Notice will inform you of the information we gather and how it is used. ABC Ltd maintains the same privacy practices with respect to data that is collected off-line and on-line and this notice also covers both those methods of data collection and use. ABC Ltd complies with EU General Data Protection Directive (GDPR) for the collection, use, and retention of all personal data. Our Data privacy Policy is available on request.

What information we gather

In general, you may visit our website without identifying yourself or revealing any personal information. ABC Ltd collects domain information from your visit to customise and improve your experience on our website.

This website may collect certain information from your visit, including the date and time of your access, the pages you have accessed, the name of the Internet Service Provider and the Internet Protocol (IP) address by which you are accessing the Internet, and the Internet address from which you linked to our site, if applicable. We use this information to better understand how our website is being used so that we can improve its performance.

Some portions of this website may request that you give us information about yourself, from which we are able to identify you, such as your name, email or other address. Some of the ways in which we may collect information from you are:

- Subscription to newsletters or other ABC Ltd content-related correspondence
- Event registrations for seminars, conferences, etc.
- White paper or other downloads

Use of the information we gather

When we collect information about you, we intend to tell you why we are asking for the information and what we intend to do with it. You will have the option of not providing the information, in which case you may still be able to access other parts of this website, although you may not be able to access certain services. In certain areas of our website, we may, where appropriate, enable you to 'opt in' to certain uses of your information e.g. personal data and direct marketing. Data will not be held for longer than is necessary, credit card transactions will be held for the duration of the transaction and general client details will be held while you are a customer.

The information we collect about you or your computer is used to run the website, respond to your requests or process any transactions you have requested. It may also be used to verify your identity, send you information or contact you in relation to an ABC Ltd product or service that you are using or that we believe may be of interest to you after you have chosen to 'Opt in'.

Sharing information with third parties

In certain instances, we may make your information available to third parties with whom we have a relationship where that third party is providing services on our behalf. We will only provide those

third parties with information that is necessary for them to perform the services and we take measures to protect your information.

The information we collect may be used, stored and processed in the EU, UK, United States, Switzerland or in any other country in which ABC Ltd does business. By providing the information via the website, you are consenting to the transfer of the information outside of your country to any country (including countries which may not have adequate levels of protection).

ABC Ltd may disclose information it has collected about you on the website if required to do so by law or when necessary to protect the rights of ABC Ltd or its employees.

Data security

ABC Ltd's intent is to strictly protect the security of your personal information; honour your choice for its intended use; and carefully protect your data from loss, misuse, unauthorised access or disclosure, alteration or destruction. We have taken appropriate steps to safeguard and secure information we collect online, including the use of encryption when collecting or transferring sensitive data such as credit card information.

However, you should always take into consideration that the internet is an open forum and that data may flow across networks with little or no security measures, and therefore such information may be accessed by people other than those you intended to access it.

How to update and/or amend the personal information you have provided

You are entitled to know whether we hold information about you and, if we do (subject to certain limitations), to have access to that information and have it corrected if it is inaccurate or out of date. To exercise your Right of Access or to update your details under your Right of Rectification or Erasure please email your request to the contact address below with proof of identity.

Business Relationships

This website contains links to other websites. ABC Ltd is not responsible for the privacy practices or the content of such websites. ABC Ltd uses pixels, transparent GIF files and other methods to help manage online advertising.

Contacting Us

If you have any questions or comments about our privacy notice or practices, please contact us. ABC Ltd may modify or update this privacy notice from time to time at any time without prior notice. You can check the "Last Updated" date below to see when the notice was last changed. We encourage you to check this notice often so that you can continue be aware of how we are protecting your personal information. Your continued use of the website constitutes your consent to the contents of this privacy notice, as it may be modified from time to time.

Email: dataprotection@ ABC Ltd.

The Framework for this notice was supplied by Atlantic Consulting

Terms of Business Agreement [CPC 2012 4.13 i)]

Data Protection

ABC Ltd. complies with the requirements of the General Data Protection Regulation 2018 and the Irish Data Protection Act 2018 (update when Bill has been passed)

The data which you provide to us will be held on a computer database and paper files for the purpose of arranging transactions on your behalf. The data will be processed only in ways compatible with the purposes for which it was given and as outlined in our Data Privacy Notice and Data Protection policy. We would also like to keep you informed of mortgage, insurance, investment and any other services provided by us or associated companies with which we have a formal business arrangement; which we think may be of interest to you. We would like to contact you by way of letter, email or telephone call. If you would like to receive to receive such marketing information please complete the permission statements contained in the Terms of Business acknowledgement letter attached.

We may receive referrals from such firms and may advise them of any transactions arranged for you.

You have the right at any time to request a copy of any 'personal data' within the meaning of the GDPR) that our office holds about you and to have any inaccuracies in that information corrected. Please contact us at dataprotection@abcltd.ie if you have any concerns about your personal data.

1 Terms of Business Covering Letter

If you want individuals to consent to direct marketing, you should have a separate unticked opt-in box for this, prominently displayed. It is good practice for firms to carefully obtain record and manage the consent to marketing obtained from their customers.

Terms of Business Effective Date xx/xx/xx
Client Name: _____

ABC Ltd. t/a Alphabet Financial Services

Status
ABC Ltd **t/a Alphabet Financial Services** ('the Company') is regulated by the Central Bank of Ireland.

Terms of Business
Attached are the Company's Terms of Business, which outline the basis on which we provide services to our clients. Please ensure that you read this document carefully. These Terms of Business apply to all business transactions undertaken for you or services provided to you and will remain in force until further notice. Should we make any material changes to our Terms, we will advise you in advance of providing any further services to you.

Privacy Policy
Here at [organisation name] we take your privacy seriously and will only use your personal information to provide the products and services you have requested from us.

However, from time to time we would like to contact you with details of other [specify products]/ [offers]/[services]/[competitions] we provide. If you consent to us contacting you for this purpose please tick to say how you would like us to contact you:

Post ☐ Email ☐ Telephone ☐ Text message ☐ Automated call ☐
I agree ☐
Customer Signature ……

We would also like to pass your details onto other [name of company/companies who you will pass information to]/[well defined category of companies], so that they can contact you with details of [specify products]/ [offers]/[services]/[competitions] that they provide. If you consent to us passing on your details for that purpose please tick to confirm:
Post ☐ Email ☐ Telephone ☐ Text message ☐ Automated call ☐
I agree ☐
Customer Signature ……

Yours Sincerely,

Joe Bloggs,
Managing Director

ACKNOWLEDGEMENTS

Brokers Ireland would like to acknowledge the contributions of the following in putting GDPR Guidance together on behalf of the members of the association:

Frontier Privacy and their consultant Aisling Clarke who engaged with us to gain an understanding of our business to ensure the Guidance would reflect both the requirements of GDPR and the requirements of other legislation and regulations relevant to the operation of a retail intermediary business.

The volunteer members of the Brokers Ireland Technical Compliance Committees and the GDPR Sub Committee who provided valuable contribution and review of the content to ensure the guidance was relevant and appropriate for members.

The contribution of member firms that enabled the participation of their staff in these committees is also gratefully acknowledged.