BROKERS IRELAND
GENERAL DATA PROTECTION REGULATIONS

FREQUENTLY ASKED QUESTIONS

FEBRUARY 2018

GDPR: Frequently Asked Questions to Brokers Ireland, February 2018.

1. Does my Firm require a **Data Protection Officer ("DPO")**?

Answer: 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 whether or not to appoint a DPO and Brokers Ireland would advise members to document the rationale for their decision.
- The criteria is as follows:-
  (i) That the core activities of your firm consist of data processing operations which require regular and systematic processing of individuals on a large scale; or

  (ii) That the core activities of your firm consist of sensitive/special categories of data (eg health data) or data relating to criminal convictions or offences.

- 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.

2. Will my firm have to delete all the **marketing leads** (i.e. prospects) built up over the years on 25 May 2018?

Answer: This really depends on whether you have sufficient consent from those leads to market to them and to do so by a particular means e.g. by email. If you have that consent, then you can.

Most likely however, you will not be sure, particularly for "older" leads. So it's recommended that:-

(i) <u>For all non-Business leads</u>:

- That you screen them against the National Directory Database (for phone) and the Edited Electoral Register (for post). Any opt outs recorded on those Registers will override any consent given to your firm.
- That when you make contact with them, eg on a date you know their insurance is due for renewal and, while offering them insurance, that you take the time to confirm with them that they consent to you contacting them in the future and by that particular means, eg phone.

(ii) For all Business leads who have contact details in publicly available Business Directories: You can continue to contact them. No change.

(iii) In the case of existing customers who have insurance with you and to whom you want to cross-sell other products: So long as you sold or renewed any insurance with them in the last 12 months or you contacted them to market insurance to them within the last 12 months and they did not request that you do not contact them for marketing, then you can continue to contact them. Confirm their marketing preferences at your next interaction.

Note Records: All marketing preferences must be recorded, i.e. a record must be kept of how and when consent was given. So, consent can be confirmed verbally over the phone but then recorded thereafter and this should be proceduralised.

3 What are the rules in relation to **data lead firms**?

Answer:

- You can continue to buy leads lists from these 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.

4. What are my obligations if I **collected the data directly** from the person? If I **obtained the data from another company**?

Answer:

- In the case of collecting data directly: Transparency about who you are & how you will use their data. Requesting consent for Marketing, Surveys, Profiling.

In the case of obtaining the data from another company eg buying marketing lists, it's best to confirm their consents before 25 May 2018 by checking them first against your own firm's database, then the National Directory Database (for phone) and the Edited Electoral Register (for address) (they may have opted out recently).

5. What happens when my IT provider tells me it is **impossible to delete or amend data** held on the firm's computer records?

Answer: This is unfortunately a common legacy issue particularly with older systems. The fact is however that your firm is already in breach of Data Protection, quite apart from GDPR. You need to seriously consider upgrading your IT or bringing in a new IT system. In the meantime, you need to ask your IT provider to what extent it's possible to delete/amend records manually or to segregate records for deletion so that at least they can't be used or to update records by means of adding a new record and somehow flagging the out of date record as 'Not For Use'. You should document this as a known risk and the actions or best endeavours you are taking so as to have it for the ODPC in the case of a complaint or an audit.

6. What can I do if information is requested on **policies in joint names**?

Answer: There are a number of points.

(i) If one of the policy holders only makes a subject request e.g. the husband of a married couple, then you can only provide him with personal data relating to himself and not his wife.

(ii) If both parties make a subject access request together i.e. in the one letter, you can provide all personal data relating to both of them in one response, i.e. you can take it that they consent to the other receiving personal data about them (e.g. health details).

Note: It's sufficient that both parties' signatures are provided.
Also: Use your judgment. It may be the case that this is simply a query which is not personal-data related, e.g. one spouse simply checking that the other has renewed the home insurance.

7. Are there special rules when handling **medical information**?

Answer: Yes. Medical information is considered a special category of personal data to which a greater duty of care applies, so for eg access levels should be more restrictive and stricter security measures in place to safeguard it. When answering a subject access request, only disclose details which are already known to the individual, so for eg before disclosing a medical report not seen by the individual, always seek the opinion of a medical professional (it doesn't have to be the author of the particular report) to confirm that disclosing it would not cause a serious risk of harm or psychological distress to the individual.

8. Am I processing **health/other sensitive data**?

- You are processing health data if you hold any data which concerns the physical or mental health of either your staff or customers.
- You are processing sensitive (or special category) data if you hold data concerning any of the following:- Health, Biometric, Genetic, Ethnic/Racial Origin, Religious/Philosophical Beliefs, Trade Union Membership, Sexual Life.

9. With whom can the firm share data in relation to **convictions**?

Answer: Any third party who needs that information for the purposes of providing insurance or a quote or to the Gardai on receipt of a court order or to a central database whose purpose is to verify penalty points information (IIDS) or to prevent fraud (Insurance Link).

10. What are the **implications for the IIDS** – (information hub for motor risks: Name, no claim bonus, previous claims convictions?

Answer:

Anti-fraud databases like IIDS (or Integrated Insurance Data System which enables brokers/insurers to verify information including penalty points and No Claims Discount (NCD)) and Insurance Link (which shares information on claims histories) are not affected by GDPR and will continue to be subject to the Code of Practice on Data Protection in the Insurance Sector. The Data Protection Bill 2018 expressly allows for the processing of criminal history data for risk assessment and fraud prevention.

11. Can insurers ask have customers **ever** had **claims or convictions** or should they restrict the period?

Answer: Yes if there is a legitimate business need, eg assessment of risk. However, the customer is not obliged to disclose any spent convictions (ie over 7 years old).
For details of the Criminal Justice (Spent Convictions & CertaIn Disclosures) Act 2016, click here.
http://www.irishstatutebook.ie/eli/2016/act/4/enacted/en/html

12. Do **named drivers** have to give consent?

Answer: No, in the sense that the onus is on the insured driver to obtain that consent.

Its important that you state this wording in the template form that you give to proposers:-
"If you provide information about someone else, such as an additional insured, you must have obtained this person's consent and have made them aware of the terms of this insurance. For motor insurance, you must also have obtained the additional insured's consent to allow us to verify their information via the Integrated Insurance Data System ("IIDS")."

13. For how long can I keep **records**?

Answer: You can only keep records for as long as you need them to provide the insurance or alternatively for as long as you are required to keep the records for legal or regulatory reasons. Your firm should have a documented Retention Schedule detailing what records you hold, the retention period for that record and the business need for it or the applicable legal/regulatory provision.

14. Is **automated processing and decision-making** still allowed under GDPR (eg generating quotes/indicative quotes)?

Answer:

Yes. But you must tell the individual when any decision-making is done purely by automated means, explaining what this is, what logic is used and in general terms how that logic can affect the decision. Also, you must inform the individual of their right to have the decision (eg a quote for insurance) reviewed by an experienced staff member.

Note:

(i) This is where decisions are made without human involvement, so it applies to online applications and not to face to face or over the phone communications.

(ii) When you inform the individual by way of wording, it must be at the point online before they submit their request for a quote (ie not elsewhere buried in legal small print).

(iii) By "experienced" staff member, this could be someone who is MCC qualified for example.

15. Is asking for **underwriting information** considered to be **Profiling** manually and electronically/on line?

Answer:

The scope of the definition of Profiling is wide enough to capture almost any analysis of an individual carried out by automated (electronic) means and in the insurance industry, this will include any underwriting processes which are performed electronically, rather than by a human being.

So Yes Underwriting means Profiling – but arguably it's essential for providing the insurance therefore an individual's consent is not required and they can't object/opt out of it being carried out.

However, Underwriting will also constitute Automated-Decision Making given that it results in a quote being decided. So Yes, an individual does have the right to know that its automated, ie that there's no human involvement, to know in general terms the logic used and how this affects the outcome and has the right to have the quote reviewed by a sufficiently senior staff member.

16. What is the difference between **Data Portability** and a **subject access request** ("SAR")?

Answer:

A SAR provides the individual on request:-
(i) A copy of their personal data held both on paper and electronically;
(ii) Is provided in hard copy or, if requested by email, by email for eg in a pdf format.

A Data Portability Request provides the individual on request:-
(i) A copy of their personal data held electronically only;
(ii) Only includes the data provided by the individual to the firm, not any data created by the firm itself;
(iii) Excludes any data provided for AML or other legal/regulatory reasons;
(iv) Is provided in an interoperable, machine-readable format eg by the individual downloading their data from a secure site using the password provided.
And
(v) At the individual's request, can likewise be provided to another Broker firm.

It's important that you inform customers of their right to make one or both of these requests and the meaning of each.

17. Am I a **data controller or a data processor**?

Answer: I'm a data controller if I control the data and process it in my own right; I'm a data processor if all I do is process it on behalf of a data controller, i.e. as an agent, eg payroll.

All Brokers are data controllers. This applies to both your customers' and employees' data.

18. Am I concerned by the GDPR? **What if I am an SME**?

Answer: All organisations regardless of size and sector are impacted by GDPR if they hold personal data. SMEs are subject to GDPR; although GDPR acknowledges the unique nature of SMEs (Recital 13), the only exemption given to SMEs by GDPR is to organisations of fewer than 250 staff to keep a Record of Processing.

Its open to the Minister to make Regulations in this area but none have been issued to date.

19. What **allows** me to process data?

Answer: You can process (hold, use) data if one of these grounds applies to your firm and its activities:-

- An individual's consent for the particular purpose (eg marketing);
- You need the data to provide a service (under a contract);
- You need the data to employ someone in your company, ie as an employer (employment law);
- You need the data to comply with a legal/regulatory obligation (eg AML documentation).

You can process special category (sensitive) data if:-

- In the case of health data, you can for your employees for employment law purposes, and in the case of your customers, you can in order to provide them with insurance;

- In the case of criminal convictions (incl. penalty points record), you need the data to provide insurance services, to carry out risk assessments and for fraud prevention.

20. **Which data** can I process (purpose)? **How much data** can I process (minimisation)? **How long** can I keep it (retention)?

- You can only process data for the purpose it was given to you, so just because you received an individual's contact details in order to provide insurance to them, doesn't mean you can use those contact details for another purpose eg marketing.
- Only use the data you need for the particular purpose, so if your Pricing Strategy dept needs customer data to analyse the proportion of drivers with over 4 penalty points your company is insuring, you need only provide them with customer numbers, they do not need the names and further details of those particular customers. This is referred to as anonymising data.
- You can keep data for as long as (i) you have a legitimate business need for it, or (ii) you are required to keep it for legal/regulatory reasons - & this should be documented by way of a Retention Schedule.

21. When is **consent valid**?

Consent is valid only when:-

- It's freely given & there's a real choice (equal bargaining power between the parties);
- It's not a term of doing business/agreeing the contract/providing the service;
- It's informed;
- It relates to a specific use/ purpose;
- It's a positive act & not assumed (no pre-ticked boxes);
- It's recorded;
- It's refreshed at least every 2 years (in the case of renewable policies only).

22. **Can consent given under the current legislation continue to be used** once the GDPR enters into application?

- Yes and for certain data you may no longer need to rely on that consent because the DP Bill gives you a legal basis instead.
- Staff data: There is now a legal basis under Employment Law.
- Customer data: There is now a legal basis in order to provide insurance.
- For Marketing to Leads: Refer to the answer to Question 2 above.. For refreshing customer consents: The ODPC's approach tends to favour using the next interaction point with the customer to confirm such preferences. Mass mail shots tend not to be productive and can lead to customer complaint.

23. What can I do with the data I collected? **Can I use the data for another purpose**?

- You can only use the data for the purpose for which it was originally received – or for a purpose that's not incompatible with that purpose.
- You cannot use it for another purpose or for one which would not reasonably be expected by the customer/staff member.

24. What is a **data breach** and what should I do in case of a data breach?

- A "data breach" is where personal data is not processed in accordance with the DP Act.
- A "data security breach" is where the security of personal data in your company has been compromised and has led to any of the following: loss, unauthorised access, unauthorised disclosure of that data.
- Certain data security breaches must be reported to the ODPC and notified to the individual(s) concerned:-
- They must be reported to the ODPC where there's a "risk" to the security of the data (so not if the risk has been managed eg by encrypting the data).
- They must be reported to the individual where there's a "high risk" to the security of the data (so for eg if their insurance application form with health

data has been emailed to the wrong third party). You do not have to notify the customer in all cases.

Practical examples of when to report to the ODPC &/or the customer:-

- 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 ie the risk to the data has been contained.
- 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, then both the DPC and the customer must be notified.
- 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.
- 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.

- The report to the ODPC must contain the following details:
    - 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;
    - The contact details of the firm's DPO or other contact point in relation to the breach.
    - (Also while not a requirement, it's good practice to include: The cause of the breach (eg, human error or systems error.)
- All reasonable efforts must be made to secure the data concerned.

25. What is meant by **Data protection by design and default**?

Answer:

- Build safeguards into your products and services when designing them.
- And ensure that default options favour privacy.

26. **What if I do not comply** with the data protection rules?

Answer:

- You can be sued by the individual(s) affected: For material & non-material loss.
- You can be fined by the ODPC: Up to €20m or 4% of global turnover.
- Even if not fined, Regulatory focus on your company by the ODPC or indeed other Regulators (eg CBI) could increase.
- You could be audited by the ODPC & they could audit you for all aspects of DP & not just for those aspects concerning the particular breach.
- You could be directed by the ODPC to take certain action(s) relating to the data you hold (in an extreme case deleting your entire marketing database).
- You could be ordered to commission a report in to particular aspects of your data processing activities and the ODPC could appoint the person to do it (or allow you to choose that person).
- You could suffer reputational damage (eg Talk Talk in the UK).

27. What is available to business in terms of **Codes of conduct, certification**?

Answer:

- Codes of Conduct: Industry sectors can develop a Code of Conduct which can then be approved by the ODPC.
- Certification: The GDPR expressly recognises certifications from approved and accredited certification bodies as acceptable mechanisms for demonstrating compliance. (There are no GDPR certification bodies in Ireland as yet. However, ISO Standards are commonly relied on and referred to.)

28. High risk processing: when should I conduct a **data protection impact assessment** (DPIA)?

Answer:

- For all new initiatives planned to be in place from May 2018 &
- Which present a High Risk (Inherent Risk, ie pre-controls) to the privacy rights of individuals OR
- Where new technology is introduced.
- Also: Where Legitimate Interests is relied upon as a ground for processing.
- When: You need to have them in place from 25 May 2018 for all new processing which satisfies the above criteria.

29. What happens if I am **processing data in different Member States**?

Answer:

- There is no difficulty transferring or sharing data with organisations (eg with other Group offices or with data processors) which are located within the EU or EEA (Iceland, Norway, Lichtenstein); they are deemed to have adequate DP standards.
- As with any transfers to other organisations, you will still need to have proper contracts in place.

30. Am I transferring data **outside the EU**?

Answer:

- You are if you are sending data to another organisation (even a company within your Group) which is located outside the EU/EEA.
- You are if another organisation outside the EU/EEA can access data held by your organisation in your jurisdiction.

- Again you will need proper contracts in place – with particular contractual clauses contained in those contracts: Binding Corporate Rules for intra-group transfers; Model Clauses for transfers to non-Group companies.

31. Am I collecting data from **children**? If yes, check age limit.

Answer:

- Yes if you are collecting data from individuals below the age of 13 (Refer Irish DP Bill).
- Note: If certain insurance contracts require parents to provide data about their children under the age of 13, their children will accrue all the rights of any other data subject at aged 14 (access etc).

32. Which measures should I take if **data are processed on my behalf**?

Answer:

- Data controllers must ensure that they carry out effective due diligence on a prospective data processor & that the contract contains the following:-

  (i) that the data processor may only process data in accordance with the data controller's instructions; &

  (ii) that the data processor must comply with Data Protection and Confidentiality; &

  (iii) that the data processor must not sub-contract without the data controller's prior permission; &

  (iv) that the data processor must notify the data controller immediately it becomes aware of a data security breach; &

  (v) that on the expiry of the contract that the data processor returns the data safely & securely & retains no proprietary rights over it.

  (Also while not a requirement, it's good practice to agree to be indemnified in the case of a data breach/data security incident.)

33. Can an **NGO/Not For Profit agency** make requests or complaints on behalf of an individual?

Answer:

- They are not entitled to make access and other requests on an individual's behalf.
- However, they can make complaint to your firm on an individual's behalf and they can appeal your firm's decision to the ODPC or take an action to the courts on an individual's behalf.

34. Is it necessary to encrypt all outgoing e mails?

Answer:

It is not necessary to encrypt all e mails**. However** any confidential or sensitive information should be attached to the email in an encrypted /password-protected document. I.e. Sensitive or confidential information should not be contained in the body of the e mail.