General Data Protection Regulation (GDPR)

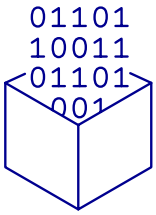
Key considerations and implications for brokers

Contents

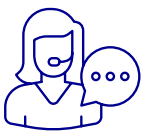
GDPR at a glance

You've probably already heard of GDPR – a new law which will regulate how personal data is dealt with, used and protected. As the impact of GDPR may vary for each business, the purpose of this awareness briefing is to highlight common themes and implications for broker directors to work with their respective compliance team or provider.

New European Union-wide data protection regulation goes live on the 25 May 2018 (and will continue to apply post-Brexit).



It will impact every single business that handles personal data.



Whilst the accountability for adoption and compliance usually sits with the management team, every customer-facing role in your business needs to be aware of the implications as the fines for breach are significant.

Why is GDPR being introduced?

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 replace existing data protection laws in May 2018.

Naturally, the world has moved on significantly since the late 90s in terms of how we use data in modern business processes, so data regulation needs to move on too.

GDPR gives additional rights for people in relation to the information that companies hold about them, obligations for better data management for businesses, and a new regime of fines if businesses don't comply.

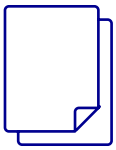
GDPR - Top 10 did you know?

1. Directors' accountability

Fines for GDPR non-compliance are up to 2% of annual global turnover (or €10million – whichever is the higher) for cases relating to control and mitigation and up to 4% of annual global turnover (or €20million whatever is the higher) for cases relating to rights and obligations. GDPR is significantly more onerous than the current data protection legislation and as directors of the business, you are accountable and responsible for the adoption, ongoing compliance and creation of supporting documentation that demonstrates your legal accountability.

2. Applies to all contractual relationships

You will need to consider carefully if you have someone doing something on your behalf, then you need to check it out, as it is likely that you will need to refresh third party contracts, as you may be accountable as the controller for lawful processing. For example, back office service providers, software houses, claims services, risk management services, HR, tax etc.



3. Paper & system records

The current and new data protection laws also apply to centrally held system back office records, as they do to personal data and consents held on paper records, historic files, files at home, mobile phones, memory sticks, local laptop documents/files etc of all employees, agents and any third party you have previously provided any client data to.

4. Pipeline marketing

From 25 May 2018, unless you have 'explicit marketing consent' for your business pipeline (e.g. lapsed customers, past quotes, cross sales, local business prospects), communicated in line with GDPR requirements (i.e. freely given, specific, informed and unambiguous) you are likely to breach GDPR.

5. Mandatory notification breaches to the ICO in 72 hours

The Information Commissioner's Office (ICO) will consider if a risk to the 'rights and freedoms' of individuals has been breached (such as leaving them open to identity theft, discrimination of loss of confidentiality). It is imperative that you have the right procedures in place to detect, report and investigate all types of personal data breaches (malicious or human error). You should consider ICO breach reporting procedures to state clearly the decision-making process in making a notification of a breach to the ICO and or to those impacted. Failure to notify the ICO of a breach can result in significant fines.

GDPR - Top 10 did you know?

6. Terms of Business Agreement (TOBA) changes

AXA has reviewed its TOBAs and identified that most of its brokers are controllers in their own right and are therefore responsible for compliance with their own obligations under GDPR. We have issued a TOBA variation which ensures your AXA TOBAs are compliant without you having to take any action. However, your other parties, for example other insurers, may take a different view. For example, you may have someone who processes data on your behalf and therefore you need to put a data processing agreement in place.

7. All clients

GDPR additional requirements and obligations are not limited to just arranging private motor, home, travel etc – they apply equally to all business customers too (e.g. personal details of owners, directors, employees etc). Being able to evidence GDPR data is processed lawfully, fairly and in a transparent manner is set at a higher standard than previously under the Data Protection Act 1998 (DPA), in that 'explicit' not implied consent is required and must be evidenced where this is used as a legal basis for processing.

8. Evidence of lawful processing

As a broker, you may be a controller (as your business may determine the purposes and means in which personal data is processed) – under GDPR you must be able to evidence 'lawful processing'; this means determining the correct legal basis for processing for all relevant types of data. You will need to analyse all your contracts to document the data flows and GDPR relationships to determine whether you are a controller or processor.

9. Customer privacy policy

Among other things, you will need to update and make available an updated privacy policy, explaining your lawful basis for processing customers' data, your data retention periods and their rights to complain. This is not an exhaustive list. The GDPR website sets out in detail all customer privacy policy considerations.

10. Training on new customers' rights

There are a range of new customer rights such as the 'right to be forgotten', 'right to portability', and 'right to object to processing' – which all of your customer-facing teams need to understand and you need to embed in your business processes (online, telephone or face-to-face). You will also need to have a clear policy on dealing with 'subject rights' for any client that wishes to pursue any of these new rights.

How to handle customer data

As you can see whilst the scope of GDPR is very broad, the compliance framework businesses will need to implement can be summarised as follows:

Treatment of Personal Data

Customer data must be handled in the right way.

Be transparent to the customer, telling them what data is collected and why

Allow customers to exercise new customer rights

Only use the customer data for the purpose for which it was collected

Ensure data held securely and lawfully

Only retain personal data for as long as legally needed

Accountability

All employees must understand their role achieving GDPR compliance.

Allocate clear responsibility (e.g. Data Protection Officer or Compliance Manager/provider)

Embed privacy when building or making changes

React promptly when things go wrong in accordance with new data protection laws

Train all employees on new customer rights and capturing consent

Maintain records and update all contracts (such as TOBAs - most insurers will issue variation updates)

Considerations for Broker Directors

The detailed table below highlights key GDPR topics and what broker directors should be considering. For clarity, this is shared for awareness only and is not an exhaustive list. As previously highlighted, it is the responsibility of each business to fully comply with GDPR.

Lawful processing / compliant contracts for data processors

GDPR Implications	Broker Directors should be considering
In controller/processor relationships, the controller is responsible for how and why personal data is processed (for which you must have a legal basis to process). Processors act on behalf of the controller and under GDPR have significantly more legal liability than before. A processor may need to appoint a data protection officer (DPO). A DPO must be independent / report into senior management. The controller must identify and document their lawful basis for processing personal data. This should also be updated in your privacy notice/policy to explain the lawful basis of processing. Brokers will need to ensure they have obtained consents where appropriate.	You should ensure that each business relationship is clearly defined, (i.e. whether you are a processor or a controller) and you have appropriate contracts in place, which deal with the onward transfer to other parties in the chain if appropriate. You will need to determine the correct legal basis for processing and, importantly, you will need to document which party is responsible for processing, including how this is technically is shared with other parties. Ideally documenting the data flow and the how and why of the data flow from one party to another assists in determining the controller/processor relationship. You should consider assigning a DPO if applicable to your organisation. You should consider reviewing and updating your privacy notice. The ICO has provided helpful tips on how to achieve this. Consent for processing personal and sensitive data in relation to Insurance Contracts now falls under a specific exemption as noted in the latest Data Protection Bill which is currently awaiting approval. However, explicit consent is still needed if you are carrying out direct marketing activities. Therefore, you may need to review your consent processes. You are accountable under GDPR to evidence that you comply with the data protection principles and procedures including setting those out in your contracts. Controllers are responsible for reviewing supplier contracts to state what a processer must and must not do with the data you supply. If a data breach occurs it will be imperative to understand if your processor has acted outside your instructions as otherwise you will be responsible for the breaches. Potential fines can be significant. Under GDPR, the ICO may choose to take action against a controller and processor if it believes both have played a role in breaching the legislation.

Considerations for Broker Directors

Consent of the data subject

GDPR Implications	Broker Directors should be considering
As noted above, when undertaking Insurance related activity the legal basis for processing will be entering into a contract (personal data) and an exemption when processing sensitive personal data. When processing outside of Insurance business you will have to rely on other legal basis, such as consent. Marketing will be a key focus from the ICO therefore obtaining explicit consent from the data subject to undertake lawful processing specifically for sensitive data or marketing purposes must be prominent in your business processes (online, telephone or face-to-face). These must be separate, clear and not hidden in wider business T&Cs. There must be a positive opt-in by the data subject (i.e. no pre-ticked boxes, use of assumptions or silence). Positive opt-in must be recorded and capable of being verified. Where explicit consent is required for marketing, you must state what data is being used and by whom (including named third-party organisations) and importantly for what purposes (e.g. future marketing). The key requirement is to provide the data subject with clear choice and to also inform them of their rights (e.g. how they can withdraw their consent), and the necessary policies and procedures to allow this. What this means from May 2018: • All direct to customer marketing activity must now have specific data subject consent (applies to both private individuals and businesses). You will need to ensure that your brokerage manages consents in a compliant way and importantly that you can evidence this.	You need to ensure that your consent processes comply with GDPR. You should review existing pipeline/marketing data sets to establish if you have the correct consents to undertake marketing activity. If consents are not verified, you may breach GDPR. Consent must be freely given, specific, informed and unambiguous. The ICO has published detailed guidelines regarding managing consents and also the wider implications of GDPR.

Considerations for Broker Directors

Data management & deletion

GDPR Implications	Broker Directors should be considering
You will need to establish and apply clear data retention policies to all data - system or manual (paper). This includes existing and past customer data as well as data sets, including marketing pipeline. Data management applies not only to data held centrally on core back-office systems (in-house or third-party platforms), but also includes local data held on laptops, mobile phones, paper records, memory sticks/CDs, spreadsheets and manual files including archive files – both in the office, at home or at any third-party premises. This also includes any business data sent to private devices. Whilst not strictly part of GDPR, if your company accepts, processes, stores or transmit credit card information, then you must also comply with the 'Payment Card Industry Data Security Standar's (PCI DSS) which has established protocols and requirements.	Establish a clear record keeping policy and regularly delete or minimise data, where appropriate and necessary. Put in place ongoing processes to adhere to the record keeping policy and retention rules (e.g. evidence through data management audits). Information held (private or business) should be sufficient and necessary for the purposes required i.e. only information required to provide the service to the customer and only kept for an appropriate length of time. You should state relevant retention period in your privacy policy.

Privacy notices & policy

GDPR Implications	Broker Directors should be considering
Ensure all your customers are notified of their new rights under GDPR in a concise, easy to understand and clear language. See 'consents' - these must be separate / prominent from your other T&Cs. Your privacy policy should be available to customers on websites, FAQs, recorded messages, emails, etc.	Create a central consistent privacy policy to inform customers in greater detail about what you do with their data. Under your privacy policy you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. This is not an exhaustive list. More information is available on the ICO website, or set out in detail within GDPR.

Considerations for Broker Directors

Individuals' rights

GDPR Implications	Broker Directors should be considering
Check your procedures to ensure they cover all the existing and new rights. For example, new rights allow the customer to request 'they are forgotten', however there are likely to be legal and regulatory requirements which will need to be carefully considered. Ensure that all of your customer-facing staff are able to respond to customers' requests and you provide clear guidance and support to customer-facing staff. Customers' new rights include: • The right to be informed, for example a clear privacy policy • The right to restrict processing • The right to object to automated decisions being made about them (including profiling) • The right of access, similar to the existing Data Subject Access rights • The right of rectification • The right to be forgotten (erasure) and the applicability of that right • The right to port data from one party to another (portability).	Include new GDPR customer rights, such as the 'right to be forgotten' and 'right to portability' and reduced timelines to handle subject access requests. Customer facing staff are likely to require training on all the new GDPR customer rights. You should also update your procedures and plan how you will handle subject's rights. You are unable to charge a fee when responding, time frame to respond to all rights is now within one month.

Allocation of accountability

GDPR Implications	Broker Directors should be considering
GDPR is likely to require a significant number of changes to your business processes. You should therefore designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. Staff training on new GDPR rules and implications will also need to be in place in advance of 25 May 2018.	Accountability forms one of the key pillars of GDPR, therefore your organisation needs to demonstrate how this is embedded within your governance. It is important that someone in your organisation, or an external data protection advisor, or an independent data protection officer, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively. GDPR is more onerous than the existing UK DPA laws. Individuals have more rights and the financial implications in failing to comply are significantly higher than those under the DPA, including the ability to pursue a class action.

Considerations for Broker Directors

Data breach

GDPR Implications	Broker Directors should be considering
GDPR makes 'Privacy by Design' an express legal requirement. A Privacy Impact Assessment (PIA) allows a business to identify and prevent future problems at an early stage, mitigating potential costs and damage to reputation which might otherwise occur. A personal data breach means a breach of security leading to the destruction, loss, alteration, or unauthorised disclosure of, or access to personal data. It is more than just losing data (e.g. lost memory stick) as it extends to data alteration (such as maliciously corrupted files) so it is imperative that you have the right procedures in place to detect, report and investigate a personal data breach. Controllers will need to inform the ICO of the nature of the personal data breach including, where possible: • The categories and approximate number of individuals and personal records concerned • The name and contact details of the data protection officer or key contact responsible in your business • A description of the likely consequences of the personal data breach • A description of the measures taken (or proposed to be taken) to deal with the personal data breach and where appropriate of the measures taken to mitigate any possible adverse effects.	A breach will need to be reported to the ICO within 72 hours of you becoming aware of it. You will need an internal breach policy to document and effectively manage the incident, undertake remedial activity and report to the ICO when appropriate. You will need to have appropriate security policies and procedures embedded within your organisation. The ICO will consider if a risk to the 'rights and freedoms' of individuals have been breached. These include potential damage to reputation, financial loss (such as leaving individuals open to identify theft), discrimination or loss of confidentiality/ social disadvantage. Where a breach is likely to result in a high risk to the 'rights and freedoms' of individuals, you will also have to notify all those impacted (remedial action may be necessary to safeguard the rights of the individual). Failure to inform the ICO of a breach may result in significant fines.

General Data Protection Regulation (GDPR)

Key considerations and implications for brokers