A BROKERS GUIDE TO GDPR

CONTENTS

Introduction

The objective of this document is to lay out in simple terms the key elements of the new General Data Protection Regulations (GDPR) and the way in which they relate to your everyday business activities and what you should be doing in order to be compliant.

Starting on the GDPR Journey

We recommend that you run through the GDPR training module on MyNACFB. Below is a link to the website that will give you access to MyNACFB or allow you to register if you have not done so already – remember access to this is one of your NACFB membership benefits!

https://nacfbcompliance.co.uk/training

In addition to this you should familiarise yourself with the NACFB Compliance resources available to support your firm's GDPR compliance. You can use the link below to gain access or register – again access to this is one of your NACFB membership benefits.

https://nacfbcompliance.co.uk/members-login-page

You will see text in RED throughout this guide – **the red indicates key 'must do's'**

The GDPR Principles cover:

- **Personal data**
- **Processing**
- **Consent**

So, you're happily working away and along comes GDPR………

Data protection is not a new concept – you are most likely to be registered already with the ICO, the organisation that regulates Data Protection (a bit like the FCA!) and complying with the (old) Data Protection Act requirements.

Times have changed mainly due to the digital world in which we live, and identity theft, financial fraud and financial crime levels have escalated enormously and the powers that be have determined that the protection of peoples' information needs to be increased to match the threats of today.

GDPR is all about PERSONAL DATA.

Personal data is defined as '**information relating to a living individual who can be identified from that information or from a combination of other information held by the data controller'.**

You as a broker at times will be a data controller, the definition of which is the 'legal' person who determines the purposes for which data is processed and the way this is done. (The data controller is normally an organisation, such as a company, partnership or a sole trader but in any event must be recognised in Law).

You will have in your firm **data processors**. The data processor is the person who processes personal data on behalf of the data controller. (If you are a sole trader you will act as both!)

It is important to recognise when you are the 'processor' and when you are the 'controller'.

For example when you pass information to a funder to consider a deal you are acting as a data controller and the funder as a data processor.

'Processing' data is defined as:

- Obtaining data
- Recording data
- Organising or altering data
- Disclosing data
- Erasing/deleting or destroying data

You process personal data as part of everyday business life and you must now consider all the activities you do that involves such information and consider it in the context of GDPR.

GDPR brings a requirement to document your business processing activities you undertake that involves personal data.

How to comply with this requirement:

- Listing all the categories of personal data that your business holds
- Document where the data is held
- Document why you hold it
- Document what security is in place for each piece of data

The NACFB Compliance website has a template you can use for this exercise and can be downloaded from the link below:

https://nacfbcompliance.co.uk/members-login-page

GDPR focusses on the rights individuals have regarding the personal data held by organisations or individuals other than themselves.

The rights of individuals cover:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to object
- Rights in respect of automated decision making and profiling

You will need to think about making sure all you do with personal data is done so with the **consent** of the individuals concerned and that at all times you consider the individual's rights.

Not only must you get this consent from each client you must also be able to evidence **how** and **when** you obtained that consent.

The best time to get a client's consent is at the start of your relationship with them – at the same time you cover your terms and conditions and fee agreements perhaps. You are going to need consent to pass details over to funders as part of the broking process so clearly it's best to get it up front. (Note also the Privacy Notice – see below - and Consent must be a separate document from your other T's and C's)

We will revisit the client facing elements a little later but first let's consider what you need to do within the business to get GDPR compliance underway.

1. You will need to either refresh your existing data protection policy or write a new one.

   Your policy will layout the way you as a firm will handle personal information – note that GDPR relates to your staff as well as clients – and reflect how you will deal with the rights of individuals mentioned above.

To help you there is a template available for you to download on the compliance website (remember if you have not registered you will need to do so to gain access) click on the link below:

https://nacfbcompliance.co.uk/members-login-page

One of the important things for you to consider is for how long you will need to keep a client's personal information on file. We would suggest that it should be for at least the term of any finance agreements you put in place plus 6 years (or any other term that you believe can be legitimately justified) – you should include a rationale for elements of your policy such as this.

Once you have produced your policy you must make sure all you do in the business complies – for example considering your 'old' client files - if you have stated in your policy that 6 years after the end of a loan agreement you will delete a client's personal information you should go back to all your records and ensure you are not in breach of your new policy!

2. Currently, you most likely refer to Data Protection in your standard terms and conditions or client agreements. You will need to refresh this document in light of the GDPR changes. That change to your document will include reference to a **'Privacy Notice'.**

   Here's an example of what you might change this element of your terms of business to:

   Privacy Notice and Data Protection

   A Privacy Notice has been issued separately from the Terms of Business. Being open and transparent and providing accessible information to you about how we will use Your personal data is a key element of the EU General Data Protection Regulation (GDPR)

   This Privacy Notice details;

   The lawful bases for processing data, who we are, how we use the information about You, marketing consent, what information is collected, why the personal data is required, our data retention periods and individuals' rights to personal data. More detailed information can be obtained on request.

   You must be confident You understand how your data will be processed.

3. You are going to need a Privacy Notice.

   The Privacy notice is a document that you will issue to all your clients and publish on your website if you have one.

   Again, the NACFB Compliance website has a template for you to use.

https://nacfbcompliance.co.uk/members-login-page

The Privacy Notice (PN) is used in conjunction with the consent you will need in order to 'process' personal information. It will set out:

- Who you are
- How you will use personal information in the context of 'Individual's Rights'
- The marketing activities you would like to carry out to the person

Your PN will be a key piece of record keeping that you will be able to evidence how and when you gained consent to 'process' a client's personal data and it may be that funders want to see that when you pass personal data across to them you are doing do with the appropriate consent.

4. You must consider all the personal data you currently hold and do so in the context of your new policy as mentioned above.

   A good place to start is to list all personal data you have and where it is and then consider if you have a legitimate reason to continue to hold that information (remember keeping and storing personal data is part of the definition of 'processing').

   For many this is going to require a disposal exercise of all those old files containing personal data for which you have no legitimate reason or consent to keep.

   In the context of the client files that you keep you must consider security of the data within them. This involves not leaving them in places that could be accessed by unauthorised personnel so a 'clean desk policy' is recommended with all paper files locked away at night. It's worth also remembering that bits of paper such as post-it notes with phone numbers or other information on could also present a risk if left around un-secured!

5. You must also consider the way you send and receive communications (e.g. via email) that contain personal data. You must ensure you make best endeavours to ensure the security of this information such as through encryption and the security of mobile devices such as phones and laptops. Note that in the event of a breach (e.g. the loss of your phone) you must be able to evidence that you had an appropriate level of protection in place.

   Regarding emails specifically, make sure that you can evidence that you have used encryption when sending personal data – unless you have a breach or a complaint you will hopefully never have to prove that you encrypted a particular email, but it will be expected that you can!

   The majority of businesses communicate via Outlook and if you use Outlook 365 you can enable encryption.

6. GDPR brings with it a responsibility to report breaches. You should have a breach reporting process and a breach notification form. This is a new responsibility!

A personal data breach is broader than just a loss of data. It means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure or, access to personal data. Breaches should be reported within 72 hours of being made aware of the breach.

So loss of a laptop or mobile phone may be a breach based on this definition.

A breach notification must detail:

- The nature of the personal data breach, including;
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the data protection officer (if applicable) or other contact point
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to deal with the breach and to mitigate any possible adverse effects

7. Summarised below (in blue) is a generic 'advice' process and on the right (in green) are the GDPR considerations that are likely to impact on your broking activities.

Introduction
- Initial Disclosure (e.g. RI and Permissions)
- **Privacy Notice**
- Terms of Business (TOB) & Fees
- Regulatory Statements
- Complaints
- Data Protection

Know Your Client
- Fact Find
- AML

Discuss Options
- Product and Solutions
- Agreement to Proceed

Recommendations
- Research Product Options
- Discuss Options with Client
- Make Product Recommendations
- Explain Product Particulars (Including Risks)
- Submit to Lender
- Contract Agreement

File Completion
- Write Client Report
- Complete Record Keeping

- Before using any personal information make sure you have a documented lawful reason for processing customer data
- If your introduction has come from a third-party source, check the introducer has the authority/consent to pass any data across
- At the earliest stage possible, provide a **Privacy Notice (PN)**, separate from the TOB and Fee Agreement which is clear, simple to understand and explains what will happen to their data? (See template **PN**)

- During the process you must inform third parties of any changes of data where possible if you know this to be inaccurate or incomplete

Record Keeping:

- Individuals must have access to their personal data and the access must be free of charge. You can no longer charge £10 for this
- Individuals may have the right to data erasure
- Ensure records are stored in a common, easily accessible format incase the individual wishes for their data to be transferred

70

8. Earlier in this guide we referred to you as the broker being a 'data controller' and the lenders to whom you pass client information the 'data processor'.

You as the broker are also a data processor (yes if you are a sole trader one person may be both!)

We have established already as a controller you need to ensure processors have consent and therefore although you begin as a 'controller' over the information you give to lenders at some stage (i.e. when a deal is agreed with a lender) the lender will become a controller too as they will begin 'processing' the data they now have on your mutual client. So you should expect that the lender will have to gain consent themselves from the client.

You will see your broker agreements being amended in order to capture this process under the GDPR, but you must remember that you remain responsible as the controller for the data you have passed to lenders that did not win the deal.

You must have a process in place to ensure that those lenders cease 'processing' and delete that data.

9. Communicating and Marketing

If you are going to market to your clients and use personal data (e.g. a personal email address) so to do, you must have the individual's consent.

Business contact information is out of scope from GDPR so you should carry out an exercise on all your marketing lists to make sure you are either communicating with a business or doing so to individuals with consent.

As a matter of 'business as usual' going forward you should be obtaining the appropriate consent (for marketing) through use of the new privacy notice. It's the mailing lists etc. that you already have that will need the checks doing. You should of course have the ability for your contacts to opt out or unsubscribe at any time.

You may therefore have to carry out a specific exercise within your business to make sure your marketing activity is GDPR complaint – you will be receiving notifications and requests for consent yourself from organisations outside your business that hold your personal data.

10. Checklist for GDPR Readiness

- Ensure key people in the organisation are aware that data protection law is changing and how it affects your business activities
- Document and review client information that you hold, where it came from and who it is shared with
- Review or create privacy notices and decide how you will use them with clients
- Check that policies and procedures reflect the rights of individuals

- Identify the lawful basis for the processing of personal data and document your rationales (or reasons) to support your decision
- Review how consent is sought, recorded and managed (e.g. for marketing)
- Review procedures to detect and report data breaches
- Designate an individual responsible for data protection compliance (if appropriate)

On the page below there is a schematic that simplifies the key elements of GDPR that will affect you as a Commercial Finance Broker.

Good Luck and remember help is only a phone call or email away!

compliance@nacfb.org.uk

Schematic:

GDPR and the Commercial Finance Deal

GDPR impacts upon many aspects of a commercial finance deal. Below is the NACFB's view on where it affects the broking process and the handling of personal data between the Client, Broker and Lender(s). This NACFB view has been arrived at after consulting with stakeholders including the Regulator. The guidance provided below is to be used for reference only, further information on GDPR can be found on the NACFB Compliance website.

Client & Broker

A. Broker provides a **Privacy Notice** to Client to process **Personal Data**.

B. **Broker's Privacy Notice** states categories of **Data Processors**, not specific Lenders.

C. Broker becomes **Data Controller**, determining how data is processed. Broker also becomes **Data Processor.**

Broker & Lender Interaction

D. With consent gained via the **Privacy Notice**, Broker approaches panel of Lenders.

E. Lenders operate under Broker Privacy Notice to consider offering.

F. Lenders cannot use Client data for any purpose other than consideration of proposal.

Broker & Chosen Lender

G. Lender is selected from panel. All other Lenders to be notified by Broker (as Data Controller) to erase Client's Personal Data (unless there is a legal requirement to store).

H. Selected Lender also becomes **Data Controller & Processor**, issuing own **Privacy Notice** to Client.

Key Definitions

Data Subject: A living person whose personal data is processed.

Data Controller: Either jointly or with others determines way personal data is processed.

Data Processor: In relation to Personal Data, processes under instruction of the Controller.

Privacy Notice: Information notice setting out how data is processed, for what purpose and by whom.

Personal Data: Information relating to a living individual that can be used (either solely or part of accompanying data) to identify that person.

Client

Data Subject

Broker

Data Controller

Data Processor

Lenders

Data Processors

Lender Selection

Chosen Lender

Data Controller

Data Processor

Broker Privacy Notice

Lender Privacy Notice

Broking & Advice Process