UK General Data Protection Regulation

(Reviewed Feb 2025)

Please Read Carefully

PLEASE NOTE THAT THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE. IT IS INTENDED TO COVER AT A HIGH LEVEL SOME OF THE MAIN (BUT NOT ALL) ASPECTS OF GDPR. IF YOU HAVE ANY SPECIFIC QUESTIONS WITH REGARDS UK GDPR / DATA PROTECTION REGULATIONS, IT IS RECOMMENDED THAT YOU SEEK INDEPENDENT ADVICE OR VISIT THE INFORMATION COMMISIONER'S WEBSITE (www.ico.org.uk)

Introduction / Overview

In 2018 data protection rules across Europe underwent their biggest overhaul in 20 years. A lot has changed since the previous data protection laws and regulations were created in the 1990s. The result was the mutually agreed European General Data Protection Regulation (GDPR), which came into force on May 25 2018. It changed how businesses and public sector organisations could handle the information of their customers.

> ***"Does Brexit Matter?"*** – In the UK, data protection is governed by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. ("***Regulations***")

These rules applied right across all aspects of your business and are not restricted to provision of finance. Whilst main focus on this document, will be 'finance' related, you should ensure that your business is compliant from an overall view.

This document is NOT INTENDED to be definitive, prescribed legal advice, but is designed to cover and create awareness on some of the key areas of data protection regulation that could potentially impact on your business. Most of the information is of a general nature and is not specifically connected to the provision of Finance (i.e. applies regardless of finance or not). Other parts of the document, do provide specific finance related guidance (e.g. section on Privacy Notices)

Contents

What are the main requirements?

Many of the Regulations' main requirements already existed within the previous 1998 Data Protection Act and EU GDPR, so if you were already complying with that, most of your approach/mind set to compliance would remain valid. However, whilst at high level some areas remain the same, with new elements and enhancements, there were changes to how you actually do things, and some things you would have to do for the first time.

Documenting Information you hold / share

You should document what personal data you hold, where it came from and who you share it with. It is recommended that you organise an information audit across your business. Regulations require you to maintain records of your processing activities.

From a provision of finance perspective, data may include (but is not limited to):

- Customer application data
- Information shared with finance providers
- Customer anti money laundering information
- Copies of credit agreements
- Declined application information

From a more general perspective, examples may include (but are not limited to):

- Customer files
- Information held on Customer Relationship Management (CRM) software
- Information relating to ancillary products / providers (e.g. warranties)
- Employee information (e.g. HR records, mobile numbers)
- CCTV records

By documenting data, and how/where it is held (be it paper, electronically or other), it is first step in demonstrating compliance with this particular area of the Regulations.

Lawful basis for processing personal data

The following is an extract lifted directly from the ICO's 'Preparing for the General Data Protection' leaflet', which provides an excellent overview on lawful basis.

> *"You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.*

Many organisations will not have thought about their lawful basis for processing personal data. Under the previous 1998 legislation this did not have many practical implications. However, this is different under the current regulations because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. You should document your lawful bases in order to help you comply with the Regulations' 'accountability' requirements."

To summarise, you should review your activities / processes and

- where consent is the basis for processing (e.g., for marketing activities), review existing mechanisms for obtaining consent, to ensure that they meet the required regulatory standards and
- where a legitimate interest is the basis for processing (e.g., sale of a vehicle), maintain records of the organisation's assessment of that legitimate interest, to show that the organisation properly considered the rights of data subjects.

Data Management (and breaches)

As a Data Controller, you have various responsibilities with regards data management. These include, but are not limited to:

- Data Security – is data held securely (electronically or hard copy)? Is access suitably restricted?
- Data retention – do you have documented processes with regards data retention? I.e. WHY are you hold data, and why are you holding it for that length of time? This will be dependent on your own business requirements (e.g. there may not be a need to retain customer web enquiries for 5 years, but there may be a requirement, for AML purposes to retain copies of customer ID).
- Data disposal – do you have documented processes in place with regards the secure destruction / disposal of data? This may relate to paper files, but also CCTV images, or electronically held data (e.g. on a CRM system)

Data Breaches

See also www.ico.org.uk

- The Regulations introduced a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Privacy Notices – General

A 'privacy notice' describes all the privacy information that you make available or provide to individuals when you collect information about them. Pre GDPR, typically this information may have been included within terms and conditions, in a 'Data Protection' clause. With current Regulations, Privacy Notices should be 'unbundled' from customer / staff terms (i.e. separate).

At very high level Privacy Notice should contain:

- who you are;
- what you are going to do with customer / staff information; and
- who it will be shared with.

If, as part of your processes, services / products are provided by another provider (e.g. a warranty company), then the privacy notice of this provider must also be made available.

It is recommended that a copy of your Privacy Notice is readily available for customers to view at any time (e.g. place on your website)

Please see www.ico.org.uk for more information and how this may apply to your business.

Privacy Notices – Finance applications

Customers must be provided with access to Privacy Notices. With a Northridge finance application for credit, this would mean minimum provision in relation to:

- The credit intermediary (dealer / broker) privacy notice i.e. your Privacy Notice
- The lender Privacy Notice (i.e. Northridge Finance)[1]. The full Northridge Privacy Notice will be generated automatically with our documents (located after terms and conditions pages) and is to be given to customer
- Credit Reference Agency Information Notice (CRAIN)[1]– Callcredit, Equifax and Experian created a standard an industry-wide Credit Reference Agency Information Notice. This provides customers with information on how their information will be used by the Credit Reference Agencies
- Fraud Prevention Agencies notice[1] - The customer personal information we have collected may be shared with Cifas, a fraud prevention agency, and will be used to prevent fraud and money-laundering and to verify customer identity

In addition, as per previous point, if you have an ancillary product or service provided by another party, their privacy notice must be made available.

Customers must be made aware of the appropriate privacy notices before application is submitted. How this is done and evidenced will depend upon your own processes, products (and additional suppliers). Appendix i provides a sample ‘script’ that can be used for guidance.

Whilst Appendix i, provides guidance in the event of finance being provided / applied for, please note that even if no finance (e.g. cash sale), your processes should encapsulate the provision of your own Privacy Notice (and any other relevant Privacy notices e.g. that of a GAP provider)

Marketing Activity / Customer Consents

The key change in relation to GDPR and subsequent UK regulations, was that customers must proactively ‘opt in’ for marketing activity (i.e. it is not acceptable to simply have a ‘tick box’ which the customer has to tick if they do not want to be contacted by you.
Marketing consents must be clear and unambiguous. Customer must also be able to select medium of any potential marketing activity (email, mail, post, text).

[1] Available to view on Northridge website at www.northridgefinance.com/yourdata

Examples of ‘opt out’ marketing (no longer possible) and pro-active opt in

We may wish to tell you about products and services which may interest you, offered by us or selected third parties. If you do not wish us to contact you with this information, please tick here. ☐ However this means that we may not be able to tell you about extra benefits available to our customers.

By ticking one or more of these boxes I am consenting to receiving information about products and services by:

Post ☐ Phone ☐ Email ☐ SMS ☐

I understand that if I do not consent this may limit the information, products and services that you can offer me.

Customers must also be advised that they can remove consent at any time, and it must be reviewed / refreshed as appropriate (e.g. if a customer purchase a car and provides marketing consent, and then returns 18 months later to purchase another car, but this time does not provide consent, you can no longer rely on the original consent)

As a business you must ensure that not only do not market customers who have not given (or have removed) their consent, and that any data on any CRM system is appropriately maintained, but you can evidence (retain) the customer’s consent.

You should also satisfy yourself with regards the difference between a marketing communication and a servicing communication and document accordingly (e.g. contacting a customer 3 years after they purchased a car to advise that there is a new model would most likely be construed as marketing and thus require customer’s explicit consent)

Other Areas that will impact

Registration with Information Commissioner's Office (ICO)

Under the legislation individuals and organisations that process personal information need to register with the Information Commissioner's Office (ICO), unless they are exempt (exemption not likely to apply to any firm that is acting as intermediary for finance). Enforcement and penalties may be applied by the ICO for non-registration

If you are unsure complete the ICO questionnaire or call the ICO helpline on 0303 123 1113

The fees for registration can be found on the ICO website

Data Subject Access Requests ('right of access')

Similar to existing legislation, customers can submit a Data Subject Access Request, to obtain a copy of all information held. Key points to note:

- Firms have currently one calendar month to respond
- The information is free to request
- Information can be requested to be sent in electronic format

Your business should have a documented process for dealing with DSARs. Additional supporting information can be found at www.ico.org.uk.

Fines for non-Compliance

GDPR has attracted media and business interest because of the increased administrative fines for non-compliance. Not all infringements of the Regulations will lead to those serious fines. The maximum fine that can be applied to a firm is £17.5mm or 4% of turnover.

Other FCA Regulatory obligations

Principles of Business (PRIN)

All firms are subject to adhering to the FCA Principles of Business, many of which will overlap with Data Protection Regulatory requirements – see highlighted in red below

1 Integrity	A *firm* must conduct its business with integrity.
2 Skill, care and diligence	A *firm* must conduct its business with due skill, care and diligence.
3 Management and control	A *firm* must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
4 Financial prudence	A *firm* must maintain adequate financial resources.
5 Market conduct	A *firm* must observe proper standards of market conduct.
6 Customers' interests	A *firm* must pay due regard to the interests of its *customers* and treat them fairly.
7 Communications with clients	A *firm* must pay due regard to the information needs of its *clients*, and communicate information to them in a way which is clear, fair and not misleading.
8 Conflicts of interest	A *firm* must manage conflicts of interest fairly, both between itself and its *customers* and between a *customer* and another *client*.
9 Customers: relationships of trust	A *firm* must take reasonable care to ensure the suitability of its advice and discretionary decisions for any *customer* who is entitled to rely upon its judgment.
10 Clients' assets	A *firm* must arrange adequate protection for *clients'* assets when it is responsible for them.
11 Relations with regulators	A *firm* must deal with its regulators in an open and cooperative way, and must disclose to the *FCA* appropriately anything relating to the *firm* of which that regulator would reasonably expect notice.
12 Consumer Duty	A *firm* must act to deliver good outcomes for *retail customers*.

Consumer Credit Sourcebook (CONC)

In addition to overall compliance with CONC, we would highlight

CONC 2.5 Conduct of business: credit broking

CONC 2.5.3 R 01/04/2019	(4) before referring the *customer* to a third party which carries on *regulated activities* or to a claims management service (within the meaning of *section 419A* of the *Act*) or other services, obtain the *customer's* consent, after having explained why the *customer's* details are to be disclosed to that third party;
	(6) bring to the attention of a *customer* how the *firm* uses the *customer's* personal data it collects, in a manner appropriate to the means of communication used;
	(7) provide *customers* with a clear and simple method to cancel their consent for the processing of their personal data;
	(8) at the request of a *customer*, disclose from where the *customer's* personal data was obtained;
	(9) take reasonable steps not to pass a *customer's* personal data to a business which carries on a *credit-related regulated activity* for which the business has no *permission* .
CONC 2.5.4 G 01/04/2014	A *firm* may comply with *CONC 2.5.3R (6)* by presenting to the *customer* a privacy notice. The Information Commissioner's Office has prepared the Privacy Notices Code of Practice.

Summary: Intermediaries should ensure not only do they have a comprehensive Privacy Notice, but customers are provided with it

Conduct of business: credit references

CONC 2.5.5 R 01/04/2014	Where a *credit broker* ("B") is a negotiator (within the meaning of section 56(1) of the *CCA*), B must, at the same time as B gives notice to a *customer*, under section 157(1) of the *CCA* (which relates to the duty to disclose on request the name and address of any *credit reference agency* consulted by B) also give the *customer* notice of the name and address of any *credit reference agency* of which B has been informed under *CONC 2.4.2 R*.

Summary: When applicable, you should provide the details of the credit reference agency (used by Northridge) (i.e. Experian Ltd, PO Box 9000, Nottingham, NG80 7WE). See also Credit Reference Agency Information Notice (CRAIN) | Experian

Appendix i - Advising Customers of Privacy Notice

The wording below is for guidance purposes only. You should satisfy yourself that your sales processes fulfil GDPR requirements (and you can evidence this). Text in red has been provided, and approved for use by Northridge, Credit reference Agencies and Cifas.

Before I go ahead and enter your details, I do need to make you aware that we are obliged to confirm your identity and permanent address. We will seek proof of your identity and address through electronic verification processes before the account is opened. We may require proof of your address if we cannot verify who you are electronically. Additionally, I must advise you as to how your personal data will be used:

- *<<Provision of credit intermediary's [dealer / broker] own Privacy Notice >>*
- We will use your data to process your application. If your application is approved, your personal data will be used for the management of your account. Full details of how your data will be used is available in the Northridge Privacy Notice document available on our website at www.northridgefinance.com/yourdata.
- In order to process your application Northridge will supply your personal information to credit reference agencies (CRAs) and they will give them information about you, such as about your financial history. Northridge do this to assess creditworthiness and product suitability, check your identity, manage your account, trace and recover debts and prevent criminal activity. They will also continue to exchange information about you with CRAs on an ongoing basis, including about your settled accounts and any debts not fully repaid on time. CRAs will share your information with other organisations. Your data will also be linked to the data of your spouse, any joint applicants or other financial associates. The identities of the CRAs, and the ways in which they use and share personal information, are explained in more detail on in the Credit Reference Agency Information Notice which is available on the Northridge website at www.northridgefinance.com/yourdata.
- The personal information we collect from you will also be shared with fraud prevention agencies who will use it to prevent fraud and money-laundering and to verify your identity. If fraud is detected, you could be refused certain services, finance or employment. Further details of how your information will be used by us and these fraud prevention agencies, and your data protection rights, can be found on the Northridge website at www.northridgefinance.com/yourdata.
- *<<Provision of any other applicable privacy notice [e.g. warranty company]>>*

[For Business Joint Applications Only - (applicant must be advised of the following information)

- If you are applying for a joint agreement and you give us information about another person, then you must have their authority to do so, and we will process this personal data on the basis that they have provided you with this consent.
- If the other party asks us to tell them who provided their information and consent to process their information/electronically check their identity, we will do so.]

Before proceeding, would you like time to fully review the various privacy notices as to how your data will be used, that is, our privacy notice, the Northridge Finance Privacy notice, the CIFAS fraud Prevention privacy notice and the Credit reference Agency information notice (and if applicable other suppliers' information notices)?

If Yes (customer would like to review privacy notices, direct to website or offer to post hard copies); if No, proceed with application