GDPR GUIDANCE FOR CONSUMER CREDIT FIRMS

Consumer Credit Compliance
info@consumercreditcompliance.co.uk

1 WHAT IS GDPR?

GDPR stands for the General Data Protection Regulation. GDPR will replace the Data Protection Act 1998 (DPA) from 25th May 2018.

2 WHAT IS THE PURPOSE OF GDPR?

Like DPA, GDPR sets out that law that governs how you collect, store, share and delete personal information that relates to individuals (clients and staff).

3 WHAT'S THE DIFFERENCE BETWEEN GDPR AND DPA?

Personal data under GDPR has a broader definition than under DPA. Under GDPR personal data includes any information which can be used to directly or indirectly identify an individual. For example, a customer reference number or staff ID number.

Under DPA, individuals have the following six rights relating to their personal information:

1. The right to access their personal data (by submitting a data subject access request (DSAR)).
2. The right to be informed about why their personal information is being collected and how it will be used. For example, through a privacy policy.
3. The right to stop the use of their personal data if it can cause damage or distress to them.
4. The right to say no to the use of their personal information for direct marketing purposes.
5. The right to say no to their personal information being used for an automatic decision. For example, an automatic creditworthiness decision.

6. The right to compensation if a firm commits a data protection breach that causes them damage.

7. The right to apply to court to get the personal information that is held about them corrected, erased or destroyed.

Under GDPR, individuals have three additional rights and have more power in relation to some existing rights. These are as follows:

1. The right to get incorrect personal information corrected without applying to court.

2. The right to get their personal information deleted without applying to court.

3. The right to restrict how their personal information is used even if it does not cause damage or distress.

4. The right to stop the use of their personal data even if it does not cause damage or distress.

5. The right to receive their personal information in a legible and transferable format. For example, in an Excel format.

Privacy policy

Under DPA your privacy policy only needs to set out your firm name, why you collect personal information and how you will use it.

Under GDPR, in addition to the above, your privacy policy needs to include who you will share the personal information with, if you will send personal information outside the EEA, how long you will keep personal information, how individuals who have consented for you to use their personal information can withdraw their consent, how individuals can complain to the ICO, whether you are collecting their personal information as part of a contractual or legal obligation and whether their personal information will be used for any automated decisions (e.g. an automatic creditworthiness assessment).

DSAR

Under DPA, you can charge individuals £10 for a DSAR and have 40 days to comply with a DSAR.

Under GDPR, DSARs are free and you have 30 days to comply with a DSAR. This 30 day time limit also applies to respond to requests to correct, delete or object to the use of the personal information.

Policies and procedures

Under DPA, it was not explicitly set out that you needed internal policies and procedures to demonstrate data protection compliance.

Under GDPR, it is expressly set out that you need policies and procedures to demonstrate data protection compliance.

Outsourcing partners

Under GDPR, you are expected to carry out due diligence on any outsourcing partners that collect and use your client and staff's personal information as part of a service agreement. You need to check that they have adequate arrangements to keep the personal information secure.

You need to make sure that your contracts include a clause to get an undertaking from the third party that they will keep the personal information that they process on your behalf secure.

Consent

Consent under GDPR has to be given by a positive action. For example, ticking an opt-in box, writing a statement or providing verbal consent over the telephone.

Pre-ticked opt-out boxes are banned under GDPR.

Breach reporting

Under GDPR, if you breach one of the requirements and it creates a risk of discrimination, fraud, identity theft, financial loss, damage to reputation of the individual this needs to be reported to the ICO within 72 hours.

ICO powers

Under DPA, the ICO can fine you for a data protection breach up to £500,000.

Under GDPR, the ICO can fine you for a GDPR breach for up to €10 million or, if you are an international company, up to 2% of your global turnover.

4 WHAT ARE THE KEY PRINCIPLES YOU NEED TO REMEMEBER?

- Make sure you are upfront to clients about why you are asking for their personal information;
- Do not use pre-ticked opt-out boxes;
- Only collect personal information for the purpose you have told clients;
- Limit the personal information you collect to only what is needed;
- Make sure you don't keep personal information longer than is necessary. This includes former staff's personal information and historic client databases;
- Make sure the personal information on your systems are up to date and accurate; and
- Make sure the personal information you keep is protected and secure.

5 WHAT CAN I DO TO PREPARE FOR GDPR?

You can review your data protection policies and procedures and check whether they need to be updated.

You can review your data processes to check that they are compliant in practice (beyond what is recorded on your policies and procedures).

You can start rolling out training to staff on the practical implications of GDPR. Our new e-Learning Course has now launched and has an entire module dedicated to GDPR. You can visit the e-Learning platform on http://www.consumercreditcompliance.co.uk/e-learning/.

Consumer Credit Compliance

Windsor House
Cornwall Road
Harrogate
HG1 2PW
01423 522599
info@consumercreditcompliance.co.uk