BLAKE MORGAN

RETAILERS AND THE GENERAL DATA PROTECTION REGULATION (GDPR):

8 PRACTICAL STEPS FOR COMPLIANCE

BACKGROUND

There has been much media coverage about the new European data protection law, the General Data Protection Regulation (GDPR), which comes into force on 25 May 2018. Brexit will not make any difference to the applicability of the GDPR and the UK Government will be tidying up the existing law in this area. It is preparing for the GDPR through the introduction of a new Data Protection Act which is expected to become law next year, having been published in draft in September 2017.

Media comment on the GDPR has focussed on the eye-watering fines that can be levied for non-compliance (potentially running into millions of Euros). However, in reality these fines will only be for very serious breaches involving large amounts of personal data and the level of fines will remain proportionate to the actual breach. Having said that, data protection compliance is important – your customers (past, present and future) and employees will expect you to process their personal data securely and in compliance with the law. The risk of reputational harm through a security breach (e.g. if customer data is stolen or corrupted or if your IT systems are literally 'held to ransom') is likely to far outweigh any possible sanctions the ICO (the Information Commissioner's Office - the UK regulator in this area) might levy on you, as seen in recent incidents with Talk Talk in the UK and Walmart in the US.

Retailers will quite rightly see the GDPR as yet another regulatory compliance burden. However, the burden is relatively light as the GDPR builds on existing law. Ensuring that you are GDPR-compliant is an opportunity to get your house in order by deleting old data and reviewing and, where necessary, updating your IT security policies and procedures.

> "ENSURING THAT YOU ARE GDPR-COMPLIANT IS AN OPPORTUNITY TO GET YOUR HOUSE IN ORDER BY DELETING OLD DATA AND REVIEWING AND, WHERE NECESSARY, UPDATING YOUR IT SECURITY POLICIES AND PROCEDURES."

Online accounts and transactions continue to grow and retailers are communicating and engaging with their customers through ever more sophisticated websites, apps and social media platforms, as well as by email, text and post. Being GDPR-compliant is not just a legal requirement – it will help ensure that your business is resilient to cyber security threats and will give your customers confidence that their personal data is safe in your hands. It will also contribute towards you being compliant with the laws on direct marketing – part of which are in the GDPR and part of which are in the separate Privacy and Electronic Communications Regulations (although the PECRs are also currently in the process of being updated) which derives from another EU Directive.

This short guide sets out 8 practical steps that you can take to help ensure that your business is GDPR-compliant.

1. AUDIT THE PERSONAL DATA THAT YOU HOLD

The GDPR only applies to personal data – information about living individuals. This can be as simple as a name, an e-mail address, a phone number and an address or as complex as HR records. However, the definition in the GDPR has also been expanded to specifically include other identifiers such as location data and online identifiers e.g. IP addresses, RFID tags etc. You don't need to know someone's name for what you hold to be considered personal data.

- Assess what personal data you hold and process in your business, and document what it is, where it came from, what you do with it and who you share it with.

This assessment/audit will form the background for the other practical steps below, as well as help you to comply with the GDPR requirement of "accountability".

It is expected that most retailers will process personal data in two main areas – (a) for marketing and sales, and (b) for internal HR purposes, including recruiting and paying staff.

2. TELL PEOPLE HOW YOU PROCESS THEIR DATA

Key to the GDPR is the concept of "transparency" – that data subjects (the people whose personal data you hold) know what personal data you collect on them and how it will be used. Your business will already be familiar with this if you collect personal data through your website or apps, as you should already have a privacy policy or notice. This will help you comply with this requirement, but the GDPR will require you to update your privacy policies/notices:

- Update your privacy policies/notices and provide additional information to data subjects including how long you retain the data, that a data subject has a right of complaint to the ICO, what the lawful basis for processing the personal data is and explaining the new rights to have data deleted, restricted or amended.
- The use of website cookies to collect and process data will also need to be reviewed, as well as explanations provided of any automated processing you carry out including profiling of customers.

The lawful bases for processing personal data in the GDPR are broadly the same as those in the current Data Protection Act 1998 (DPA 1998). For example, where the consent of the data subject has been given, where it is necessary for you to process the personal data (e.g. payment details, an address) in order to fulfil a contract (e.g. to complete a sale or deliver the goods or services to the customer), where you have a legitimate interest in so doing, etc.

Also, you need to be particularly careful if you (a) acquire personal data from third parties (e.g. by buying in marketing lists or getting redirects through affiliate marketing programmes – this is high risk), or (b) share personal data about your customers with others. Issues of transparency will arise but also issues of consent (see 4 below).

The GDPR also now specifically requires you to give individuals detailed information where you have not obtained the data from them direct but via a third party. This includes telling them where you get their data from.

3. BE ALERT TO THE RIGHTS OF DATA SUBJECTS

The GDPR gives data subjects a number of important rights. These are similar to the rights that already exist under the DPA 1998, but have been enhanced. Some of these rights e.g. the right to data portability (to have your personal data given to you or to others at your request in a machine readable format) have received much media coverage, but are likely to be less relevant to retailers. Others, such as the right to be forgotten (to have personal data erased) may be more relevant:

- Ensure that you are able to respond to requests by data subjects to have their data corrected, erased, to stop the processing of their data (e.g. for direct marketing) and to have access to their data (data subject access requests (SARs)). In particular you cannot now charge for responding to SARs and you only have a month to comply.

> "KEY TO THE GDPR IS THE CONCEPT OF 'TRANSPARENCY' – THAT DATA SUBJECTS KNOW WHAT PERSONAL DATA YOU COLLECT ON THEM AND HOW IT WILL BE USED."

There is also a specific new right to object at any time to the processing of personal data for profiling purposes where you are relying on legitimate interests as your ground for processing. You must stop processing data, if so requested, unless you can demonstrate compelling legitimate grounds to keep doing so. However, if the processing is for the purposes of direct marketing (including profiling for these purposes), retailers will not be allowed to justify continued use and must stop immediately.

If your customers are subjected to any automated decision making process, this must be explained to them as mentioned above and individuals must also be allowed to object to that process. If the process is required for the purpose of a contract (e.g. to decide if you will sell them a product or allow them credit) or is based on an individual's consent, retailers must also:

- Implement suitable measures to safeguard individuals' rights which, at the least, must include a right to obtain human intervention in the decision making process, a right to express their views on the process and a right to content the decision.

4. REVIEW HOW YOU OBTAIN CONSENT AND ENSURE THAT THE PERSONAL DATA YOU HOLD IS UP TO DATE

One of the most commonly used lawful bases for processing personal data is consent (i.e. the data subject has consented to what you want to do with their data). Under the GDPR consent must be freely given, specific, informed and unambiguous. You cannot infer consent from silence or pre-ticked boxes and sections on consent must be clearly separated from other text and split up to make it clear what is being consented to. Sweep up or general consent wording is not permitted.

Also, if you decide to rely on consent, the data subject can revoke their consent at any time. Retailers will often use consent as the legal basis for permitting the direct email marketing of customers.

- Use the GDPR as an opportunity to check that you have the required consents in place (e.g. for direct marketing) and that the information that you hold is accurate, is not excessive, is up to date and is not kept for longer than is necessary.

As mentioned above, the rules relating to opt-ins and opt-outs are dealt with in Regulations separate to the GDPR and there is currently uncertainty about whether or not these rules will stay the same. However, it appears likely that the rules around cookies, Wi-Fi location tracking and other similar device tracking and in-app adverts etc will become tighter than they are at present. The rules may require consent to the use of these tracking methods to be obtained on the same basis as consent is obtained under the GDPR. Suggestions have also been made that so called "cookie walls" (whereby people cannot browse a website without accepting cookies) should be banned.

5. TAKE IT SECURITY SERIOUSLY

A fundamental requirement of the GDPR is that the personal data that you hold and process must be appropriately protected against unauthorised or unlawful processing and against accidental loss, destruction or damage "using appropriate technical or organisational measures." This is a deliberately vague requirement as there is no one size fits all approach to IT security. What is clear is that you must put in place an appropriate level of security having regard to what you process and the risks involved. The nature of banking and credit card data or sensitive HR data demands a higher level of security (such as encryption) than just a telephone number, for example. This is not a new requirement. What is new is that data breaches in relation to personal data must in the majority of cases be notified both to the ICO and to the data subject. A personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". This is a very broad definition which could encompass, for example, hacking, losing a memory stick or a laptop containing personal data or suffering a malware or ransomware cyberattack where personal data is corrupted or encrypted.

- Use the GDPR as an opportunity to review your IT security and policies. Be aware that in most cases you will have to notify the ICO of any personal data breaches within 72 hours after becoming aware of them and if the breach is high risk then you must tell the data subjects affected as well "without undue delay".
- Check if your insurance policies are sufficient to cover any possible liabilities that might arise.

6. REVIEW YOUR IT AND DATA PROCESSING CONTRACTS

You cannot contract out of the GDPR by using someone else to process personal data on your behalf (e.g. by using a service like MailChimp to manage marketing emails). You as data controller remain primarily liable for GDPR compliance although the data processor you appoint will also be liable as well. Where you appoint a data processor you must do so under a contract containing certain required safeguards (e.g. as to security and how the data will be processed). Also, if you are "exporting" personal data outside the EEA (e.g. to a processor in the USA), then this will not be lawful unless certain additional safeguards are in place as well. You may think that this is not likely but most cloud platforms rely on servers dispersed around the world and use of these platforms is very likely to mean that you export data outside of the EEA

> "A FUNDAMENTAL REQUIREMENT OF THE GDPR IS THAT THE PERSONAL DATA THAT YOU HOLD AND PROCESS MUST BE APPROPRIATELY PROTECTED AGAINST UNAUTHORISED OR UNLAWFUL PROCESSING..."

- Review whether or not you use any data processors. This is likely if, for example, you use an email marketing service, an online HR platform or outsource any part of your IT platforms. Having done this, consider whether the contracts that you have with data processors are up to date in imposing certain key requirements on the data processor required by the GDPR? Also, check if any personal data is exported outside the EEA. If it is on what legal basis is this permitted?

You are also responsible for approving and checking any sub-contracting undertaken by your data processors. Check whether or not your providers – particularly IT providers – rely on a larger provider such as Microsoft or AWS.

7. TAKE PERSONAL RESPONSIBILITY FOR GDPR COMPLIANCE

You are more likely to comply with the GDPR if all those in your business are aware of the basic rules around the collection and processing of personal data. It is also sensible, depending on the size of your business, to appoint someone to take responsibility for data protection compliance. Note that the GDPR requires certain sorts of organisations to formally appoint "data protection officers". However, these rules are unlikely to apply to retailers unless you process data on a large scale to monitor data subjects (for example, by collecting geo-location data on customers through an on-line shopping website or app, or an in-store web beacon which relates to your core business activities or offering certain sorts of loyalty programmes). If you are not obliged to appoint a data protection officer you may still wish to appoint a person responsible for data protection compliance nonetheless.

- Raise awareness of data protection in your business and depending on your size consider appointing a member of staff with responsibility for this area. In certain cases, you may need to formally appoint a "Data Protection Officer".

8. REVIEW YOUR EMPLOYMENT PRACTICES, PROCEDURES AND CONTRACTS

Retailers will have access to and will process HR data. This means that the above steps will also apply to this information. Note that employers cannot in general rely on the employee's consent alone as a legal basis for processing employee data. Other grounds need to be found due to the imbalance in the relationship between employers and their workforce. The GDPR will impact on employment practices and procedures as well as HR contracts and policies.

- Do not forget that the GDPR also applies to HR data. The law will need to be complied with when recruiting, managing, training and paying staff. HR documentation including employment contracts will need to be updated to reflect the GDPR.

"YOU ARE ALSO RESPONSIBLE FOR APPROVING AND CHECKING ANY SUB-CONTRACTING UNDERTAKEN BY YOUR DATA PROCESSORS."

BLAKE MORGAN

FURTHER INFORMATION

Please contact the author, Sheilah Mackie, Partner, Blake Morgan for further information on how to comply with the GDPR:

☎ 023 8085 7039

✉ Sheilah.Mackie@blakemorgan.co.uk

www.blakemorgan.co.uk

Blake Morgan LLP, New Kings Court, Tollgate, Chandler's Ford, Eastleigh, SO53 3LG