LEWIS SILKIN

Top 5 GDPR issues for... retailers

With the EU General Data Protection Regulation ("GDPR") looming on the horizon, we take a look at some of the key changes of how this legislation which will affect retailers from 25 May 2018.

1. Consent

Ever purchased something and been asked for your email at the till so you can receive an e-receipt? What was then sent through? A receipt or also some vouchers to purchase additional products? A common use of customer personal data is for marketing purposes and if retailers want to collect emails from customers in store so they can send customers new deals, or other marketing materials later (rather than a simple e-receipt), the retailer will need the customer's consent.

Under GDPR retailers will need to ensure an individual's consent is fully informed, actively and freely given. Consent won't be valid if the details about why personal data is being used is hidden within a long set of terms and conditions provided to a customer. GDPR explicitly requires retailers to call out the consent clearly and as a stand alone provision. Pre-ticked boxes are not allowed. Form-based consent may still possible but retailers will need to ensure consent forms whether in paper copy instore or online, contain appropriate data capture language to clearly explain the data use.

Retailers should also bear in mind that the potential changes to data capture language or customer facing documents won't be the only consent they need to review. GDPR has codified previous guidance that consent by employees won't be valid as it's not freely given in an employment context. Retailers should therefore also consider whether they're currently relying on consent from employees to process employee personal data, and consider the alternative grounds which can be relied on.

2. Profiling

GDPR also regulates profiling of individuals and introduces a new definition of "profiling" which includes where data is collected in an automated form and used to predict or analyse personal preferences of a customer. Retailers profile customers in a number of ways, whether through the use of loyalty cards, online behavioural advertising or using CCTV to record instore images of known individuals.

Where a retailer chooses to profile an individual and that profiling has a "legal effect"on the individuals, under GDPR this will only be possible with consent (unless the profiling is necessary for you to deliver the 'contract' with the customer). If there's no "legal effects" then you can profile, provided that you have told customers about this and give them the opportunity to object. "Legal effects" are not defined so to some extent will be guided by the regulator's interpretation, but by way of example, first party behavioural advertising is unlikely to have a legal effect but profiling using loyalty card data and then restricting deals offered to a particular customer may well have a legal effect.

Note that the profiling requirements under GDPR are separate from the current e-privacy rules ('PEC Regs') which still require you to obtain consent to placing cookies on an individuals' device. If your profiling is achieved via cookies, consent may already be in place, provided the rules mentioned above were followed. It should be noted that the European commission have also recently issued a new draft E-Privacy Regulation which is intended to replace the existing e-privacy rules, at the same time as GDPR is implemented.

3. Security and data breach notification

Security requirements are imposed on both retailers and their data processor suppliers under GDPR. This is a change from current law where suppliers simply have to agree to comply with the relevant retailers' security requirements and don't have direct liability. In addition, GDPR introduces mandatory data breach notifications to the regulator within 72 hours and in some cases to the data subjects too. Up to now, unless an organisation is already caught by the PEC Regs data breach requirements, notifications have been voluntary.

Retailers need to give very careful thought to breach prevention and to ensuring that breaches are handled in the right way. This will not only help avoid non-compliance but reduce the risks to the business of bad press and any subsequent customer and/or profit losses which could result from a data breach. Some of the most public recent data breaches have involved retailers and there are, sadly for the retail sector, plenty of examples to choose from.

Retailers should consider how an actual breach will be handled. Different procedures might be in place if a complaint comes in via a customer service call or email than if the retailer discovered the breach internally through, say, its own IT system. Either way, retailers should consider who else might need to be involved: insurers; PR agency; other suppliers; and should raise awareness among all the workforce and train staff as to appropriate behaviour and procedures. Retailers should also implement a joined-up approach across multinationals, as a breach may concern more than one jurisdiction.

4. Data processing arrangements

Retailers will use a number of suppliers and those handling personal data will be processing that data on behalf of their retailer client. For example, delivery or logistics providers delivering to customers as well as marketing agencies will be data processors. The existing requirement to have a written processing agreement in place with all data processors continues under the GDPR, but there are more prescriptive requirements as to the content of those agreements. In addition, as data processors have their own direct obligations under GDPR for the first time, it's likely that data processing agreements may be more negotiated than in the past.

Existing arrangements with all processors should be reviewed and updated where necessary. Processing agreements will need to detail the security measures required as well as set out obligations on the processor to assist the retailer in the event of a data breach and/or any request by a data subject to exercise their rights to access or the new right to data portability.

Although most agreements with suppliers will be data processing agreements, retailers may also share data with third parties who are also data controllers. For example, rewards under a loyalty programme might involve a customer's data being shared with the applicable "reward" provider. Such an arrangement is more likely to be a data sharing, and not processing arrangement. That doesn't avoid the need for an agreement to be in place but the requirements differ and the ICO's Code of Data Sharing should be considered too.

5. Cross border data flows

Identifying international flows of customer and/or employee data, whether internally within the retailer's group of companies or with third party suppliers, is an essential part of preparing for GDPR compliance. Retailers operating stores or online sales cross-border should already be complying with the rules on international data transfers under current law which remain similar under GDPR, although recent development such as the EU-US Privacy Shield and challenges to EU approved Model Clauses means they will need to keep an eye on these relationships particularly as the UK withdraws from the rest of the EU.

In addition, the GDPR introduces a new concept of the "lead regulatory authority" who will deal with complaints and sanctions where a retailer is processing data across EU-borders. A retailer's lead regulator will be the country where the controller or processor has its main establishment and this can vary depending on the type of data involved (for example one group of companies might centralise its marketing function in the UK, but run all its supply and procurement relationships from France).

Why does it matter?

Although much of the GDPR codifies existing guidance from the EU regulators, the changes being introduced are intended to introduce a new mindset and culture shift in relation to the use of data. While regulators will still have the ability to discuss issues with organisations and individuals and ask for undertakings or commitments, the financial penalties of non-compliance are exponentially increasing up to a maximum of the greater of 4% of global turnover and Euros 20 Million this level of fines is necessarily drawing the attention of the board room to data protection compliance.

For retailers, a particular challenge of GDPR is to ensure that essential customer relationship management is not affected by the more prescriptive changes required under GDPR and that customer trust is maintained at all times.

This note is not intended to be an exhaustive list of GDPR changes so if you require any further information or advice about this subject please contact:

Olivia Savage
Managing Associate

+44 (0) 20 7074 8231
olivia.savage@lewissilkin.com