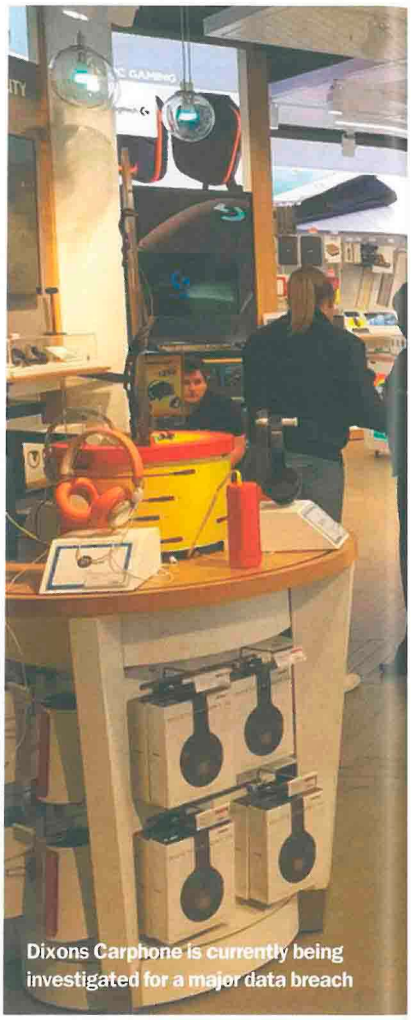
NEED TO KNOW

How GDPR is impacting retail

The new data law has had serious repercussions on UK retail, including a surge in data requests and the looming threat of legal action. **Matthew Chapman** reports



Dixons Carphone is currently being investigated for a major data breach

Surge in data requests

GDPR is placing administrative strain on retailers because of the ease with which it is now possible to make a subject access request.

A subject access request allows anyone to ask what data a company holds on them.

Under GDPR, retailers are forced to respond in 30 days. People are no longer charged a fee for making the requests and can ask for their data to be deleted.

"It is coming as quite a shock to clients because they've not had to deal with that sort of process before nor the volume," says Robert Bond, partner and notary public at law firm Bristows.

"They are struggling to deal with the volume and to do it in the time and to understand whether they really have to erase everything."

Clients are struggling to deal with the volume and to do it in the time and to understand whether they really have to erase everything
Robert Bond, Bristows

Bristows has recently had to deal with a case where a customer wanted all their records deleted, which would have conflicted with the retailer's requirement to keep certain data for warranty purposes.

Bond estimates the clients he is dealing with have seen a 50% increase in subject access requests since GDPR. This is on top of a big increase in the requests being made prior to GDPR as consumers become more aware of how their data is being used and their rights.

It appears there could still be some teething issues with how retailers are currently dealing with the requests.

A Retail Week staff member submitted a subject access request to Tesco, which the retailer failed to respond to within the 30-day deadline.

When Tesco did respond it said it could not provide the data unless Clubcard details were provided. This requirement was impossible to comply with because the consumer had no Clubcard.

International retailers stop selling into UK

Brands snapped up in Walmart's recent acquisition spree are no longer selling into the UK.

Any UK visitors to the websites of Bonobos, Modcloth, Moosejaw and Shoes.com are met with a near-identical message. It reveals the Walmart-owned companies are no longer offering products to EU/EEA countries because of GDPR.

Walmart is not the only retailer that has decided to alter its operations as a result of GDPR.

Beauty specialist Sephora now directs its UK and Dutch customers to its French rather than US website. The change has caused consternation among customers because the retailer's French website does not stock as many products and has a different loyalty points system.

However, the decision of some non-EU retailers such as the Walmart brands to stop selling in the region could be more the exception rather than the rule.

Bond says none of Bristows' US retail clients have taken the Walmart approach yet.

Walmart's decision to block EU customers from buying from its brands is puzzling because of its experience of operating in the UK through Asda.

Sacha Wilson, partner at law firm Harbottle & Lewis, believes the decision could be influenced by the potential levels of liability it could face.

"Even if one entity within a group isn't caught but another one is, the assessment of the fine of the one that is can be against the whole group," explains Wilson.

The GDPR can theoretically lead to fines of up to 4% of revenues. Based on its most recent annual revenues of $500.3bn, Walmart would be potentially liable for a $20bn fine if it was found to have broken GDPR. The likelihood of such a fine is extremely small, however, because the UK's data regulator has hinted it will take a pragmatic approach.

"The Information Commissioner's Office (ICO) has been very vocal it will not increase fines disproportionately just because there is a theoretically much higher maximum fine under the GDPR," says Wilson.

However, other regulators in EU member states could take a more robust approach.

France's CNIL regulator and some of the regional German data protection authorities have a reputation for being much more conservative in their interpretation of compliance and are more aggressive in their enforcement.

Wilson speculates that other factors playing into the Walmart decision could be fears about the additional administrative burden of complying, and concerns that GDPR could restrict how it uses data for its marketing activity.

And even if US retailers do not comply with GDPR now, they could

For the latest retail data and analysis
Retail-Week.com/Data

Sephora is directing UK customers to its French website

Walmart is blocking EU customers from buying from its brands

be compelled to deal with strict data privacy regulations in future.

GDPR has already influenced lawmakers elsewhere and will soon impact Walmart's home country.

"California has introduced laws around the Consumer Privacy Act 2018, which comes into effect in January 2020, which people are saying is actually more stringent than GDPR," says Oli Freestone, principal at consultancy Elixirr.

Marketing concerns

How retailers are grappling with the use of data in digital marketing is a key concern for retailers internally, according to Wilson.

"The retail sector has some of the most poorly governed internal marketing teams that I've seen," says Wilson.

"A lot of in-house legal counsels are trying to get more visibility on what their digital marketing teams are doing, particularly on social media, and GDPR has focused their minds.

"Retail generally has been a bit laxer in the way it has done its digital marketing and the teams will do anything without good governance and internal regulation of what they are doing."

The retail sector has some of the most poorly governed internal marketing teams that I've seen
Sacha Wilson, Harbottle & Lewis

Threat of suits and fines

The threat of potentially eye-watering fines under GDPR are well documented, and on top of that retailers could also be faced with the additional financial risk of class action lawsuits.

Retailers will have their eyes on a couple of potential test cases when it comes to the levels of fine under GDPR.

Major data breaches at Ticketmaster and Dixons Carphone are currently being investigated, and the ICO is yet to announce if the breaches will be dealt with under the more stringent GDPR rules.

"That will be an acid test on how heavy the ICO will come down, what the fines will be and that might set the precedent," says Freestone.

If the ICO does end up taking a more pragmatic approach to GDPR fines then the greater financial risk could potentially come from the emergence of "quasi class action lawsuits".

Bond predicts that GDPR could encourage the public to take up the services of 'no win, no fee' lawyers that will target companies that have suffered a data breach.

This could have serious financial implications. A precedent has already been set when a court ruled that Morrisons was liable for a data leak – which occurred before the implementation of GDPR – about staff and would have to offer them financial compensation.

"We are still waiting for the court to come out with the quantum of damages that Morrisons will have to pay to every employee," says Bond. "It could be £10 or £1,000 for each employee. What if it was not just 3,000 people affected but 3 million?"

The level of fine in the Morrisons case could make data breach lawsuits a very profitable pursuit.

Upside

The introduction of GDPR is causing retailers many challenges, and is likely to continue to do so while they streamline their procedures and audit their practices.

More stringent data regulations need not only be seen as a negative, though; they also provide opportunity. Retailers are acting to get their houses in order and truly understand their data.

When they do that they can put it to good use to ensure they are benefiting not only themselves, but also the customer. RW