Ready

The new GDPR legislation is here, tightening up rules on data retention and use – and bringing with it the threat of significant fines for those companies that fail to comply. Is your business prepared?

Andrew Don

This week sweeping new regulation comes into force in the UK transforming the rights, rules and risks that surround handling data.

Imported from the EU rulebook, the General Data Protection Regulation (GDPR) leaves all businesses vulnerable to fines of up to 4% of turnover or €20m (£17.9m) – whichever is highest – for failure to comply with the new obligations around the collection, storage, and protection of personal information.

With much of the UK food and drink market dealing directly with the public on a daily basis, be it through card payments, loyalty schemes, or online registration, as well as employing more staff than nearly any other sector, the ramifications could be huge.

Yet as the deadline hits it's estimated that only 40% of businesses are fully compliant. So, what are five ways GDPR could directly affect the grocery sector? And how can businesses prepare?

Protect against cybersecurity breaches

Though there is no material change under GDPR regarding the steps an organisation is expected to take to protect against cyberattacks, says Martin Sloan, partner in the commercial services division at Brodies, the legislation does introduce sanctions for failing to meet current standards or report breaches.

All businesses must therefore ensure they have 'appropriate security of personal data' and notify the Information Commissioner's Office within 72 hours if that security is breached. Failure to do so could incur fines of up to €10m.

Emma Burns, partner and head of employment law at Hugh James, points to the recent Morrisons case, where disgruntled employee Andrew Skelton leaked the payroll data of nearly 100,000 staff, including names, addresses, bank account details and salaries, demonstrating that internal security is just as important as protecting against external threats. In fact, "one of the main causes of breaches is staff ignorance or carelessness," she adds.

"One of the main causes of data breaches is staff ignorance or carelessness"

An organisation suffering a cybersecurity breach will need to move quickly to identify, contain and investigate, and decide whether the breach is one that needs to be notified to the ICO, says Sloan. The breach may also need to be notified to the individuals affected.

Practical steps to prepare

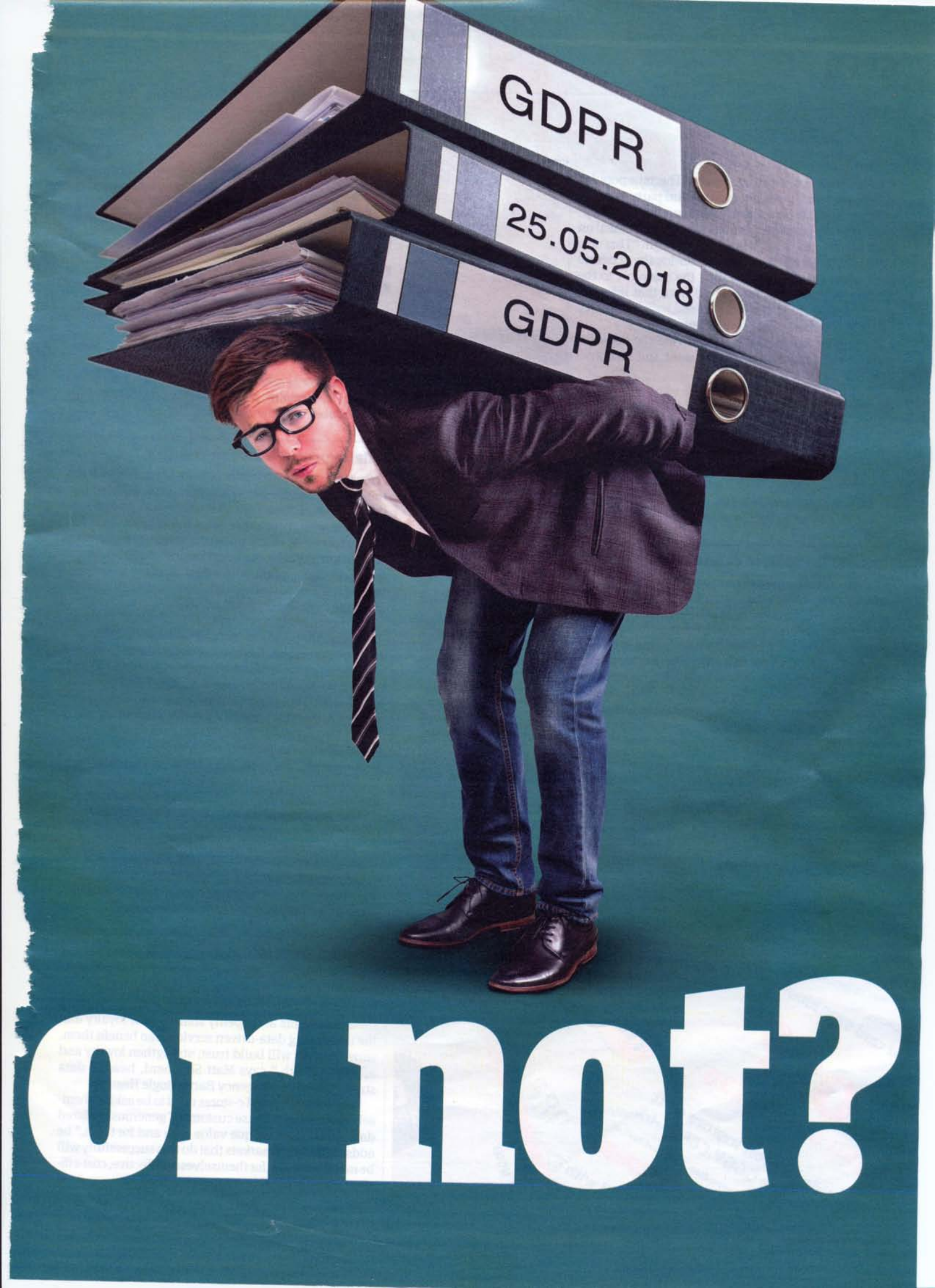
- *Implement policies and procedures to protect against, and mitigate the impact of, cyberattacks*
- *Put in place a policy for handling personal data breaches, of which all staff are aware*
- *Regularly refresh training to reflect any changes*
- *Adopt a Breach Notification Procedure*

Provide consumers with access to data derived from loyalty schemes

Under existing UK law all consumers already have the right to make 'subject access requests' to view information held about them – though few are aware of it. Under GDPR not only has that right become far more heavily publicised, but it is no longer possible for businesses to charge for that information – and the time for handing it over has been cut from 40 calendar days to 'within a calendar month.'

More significantly for retailers running loyalty schemes, there is an entirely new right created by GDPR, which applies where personal data has been shared on the basis of consent, for example through signing up for a store card, and is stored electronically.

Get the full story at thegrocer.co.uk


GDPR
25.05.2018
GDPR
or not?

Requesting access to this data could become popular if, as expected, it gives rise to new third party services offering to collate personal data on spending and shopping habits to provide consumers with a better deal on their weekly groceries. It is limited though. "This new right will likely apply to data under loyalty schemes but only to the data provided by the customer to the retailer and not any data derived from that information," explains Ruth Weir, associated solicitor, corporate and commercial at Blackadders.

To comply, businesses must provide the personal data in a structured, commonly used and machine-readable form.

Practical steps to prepare

- *Inform consumers of their rights when collecting personal data in a clear online privacy notice*
- *Adopt a formal process for dealing with requests*
- *Provide clear training on different ways someone might make a request*
- *Include as part of training the right person to notify when a subject access request is made.*

Ensure all employee data is open for scrutiny

GDPR requires far greater transparency around the processing of employee data, warns Sloan. In particular, employees will have the right to be informed about how their personal data will be used, the right to access data and the right to be forgotten from the business records, explains Dave Halford, sales director at customer service outsourcing business Echo-U, which works with HelloFresh, Asda and Tesco. The 'right to erasure' means a person can request their data is removed or deleted from a company database when there is no compelling reason for them to have it. And it's been estimated that up to three quarters of employees might exercise this right, according to a survey by Clearswift, with 48% of businesses concerned this could have serious consequences by virtue of the administrative resources involved in processing a request.

Practical steps to prepare

- *Carefully review how employee data is currently used, particularly in relation to monitoring*
- *Ensure any monitoring carried out is fair and lawful*
- *Ensure an accurate register of any data processing activities and use impact assessments to demonstrate compliance*
- *Take the time to review employee information including recruitment records, performance reports, any training undertaken and payroll statistics.*

Obtain consent before any contact

A requirement for all businesses to 'prove consent' for the host of data they hold is a significant pillar of the new GDPR regime and one that will require proactively engaging with a customer base. Information held for the purposes of email updates, newsletters, loyalty schemes or any other such service now require consent to be actively supplied, with a number of organisations having reached out to their database ahead of the GDPR deadline to ensure it was obtained.

For Jason Palgrave-Jones, MD of SMS platform Textlocal, "implied consent can no longer be enough. Any customers ordering with your business must provide their personal data to complete an order; but any further communications must be a marked decision by the user. This means customers must tick a box to say yes, rather than untick a pre-filled box to say no."

Practical steps to prepare

- *If engaged in electronic marketing, review current consents and identify any potential risks*
- *If asking subscribers whether they wish to continue receiving information, only contact those who have given current consent*
- *Third party-sourced mailing lists should be used only with caution and after detailed diligence on what consents were obtained*
- *Review and update any data capture forms including opt-in/opt-out boxes, and privacy statements*

Finally... seize the opportunities

Though GDPR has been portrayed as at once hugely complex and potentially costly, there are opportunities. For one "by proactively informing shoppers about their data rights and openly sharing how loyalty and the underlying data-driven services can benefit them, supermarkets will build trust, strengthen loyalty and achieve growth," says Matt Shepherd, head of data strategy at creative agency Bartle Bogle Hegarty.

"Supermarkets and c-stores need to be asking themselves how they will use customers' generously offered data to co-create unique value with and for them," he adds. "The supermarkets that do this successfully will be manufacturing for themselves an effective, cost-efficient and sustainable competitive edge."

GDPR could impact the ways in which retailers must store and share data collected via in-store loyalty schemes

Get the full story at thegrocer.co.uk