THE GREAT DATA BALANCING ACT

THE INTRODUCTION OF THE GENERAL DATA PROTECTION REGULATION REQUIRES MUCH OF BOTH TREASURY DEPARTMENTS AND THEIR BANKS, REPORTS GRAHAM BUCK

Another in a series of long-anticipated deadlines is upon us. Friday 25 May is the date for compliance with the EU's General Data Protection Regulation (GDPR), when more than 200 pages of data-privacy regulations will impact on how companies manage, process and delete data. GDPR applies to all of the 28 EU member states, and aims to both standardise and strengthen data protection for all EU citizens (even when they reside in a non-EU country), while also regulating the export of personal data to non-EU countries.

At its heart, the regulation is about transparency and accountability when it comes to the gathering and use of personal data, says Fedelma Good, a director of PwC's data protection practice.

"The GDPR is an evolution in data protection, not a revolution, and it seeks only to build on the existing principles that have been in place for the past 20 years, including fairness, transparency, accuracy, security, minimisation and, above all, respect for the rights of the individual whose personal data is being processed," adds Good.

"These are all principles that any organisation processing personal data should already be aware of and adhering to. The GDPR demands more of organisations in terms of accountability for their use of personal data and enhances the existing rights of individuals in relation to that personal data."

Any company, regardless of its location, that holds data on EU citizens must comply with the GDPR's requirements. This means banks, together with other organisations that conduct identity checks and hold sensitive information about customers, are required to be completely transparent on what happens to this data once it has been used.

The government has agreed that UK law will align with the GDPR, which is being transferred into the Data Protection Bill. Banks and other financial services providers have had the task of assessing and refining their methods of handling customer data so that they satisfy both the GDPR and KYC processes. KYC goes beyond just the onboarding of a new client, as the information requires regular maintenance and updating as and when appropriate to ensure that it continues to be valid.

Banks and insurers have long demanded some form of verifiable information to prove that the customer is who he/she says they are (or the directors/authorised signatories where the customer is a company) – typically in the form of a passport or driving licence – in order to comply with anti-money laundering measures and prevent other forms of fraudulent activity. However, the GDPR raises the question of whether there are other means of providing the information that don't involve having to hand over an item proving ID.

"One of the key issues for KYC due-diligence processes is consent," notes Susannah Hammond, a senior regulatory intelligence expert for Thomson Reuters. "The basic concept is that consent is required as a lawful basis (or condition) for processing personal information. While the concept of consent

IKON IMAGES

and the surrounding rules was in previous iterations of data-protection legislation, the GDPR contains more detail and codifies existing guidance and good practice.

"The GDPR sets a deliberately high standard for consent with the expectation that firms will have clear, granular opt-in methods, good records and simple easy-to-access ways for people to withdraw consent."

That said, companies are allowed to insist on collecting personal data providing it is core to offering the service, ie they can refuse to provide that service if the customer refuses to allow data to be collected and stored.

Muddying the waters?

However, the GDPR challenge has been given added complexity by other recently introduced legislation. This includes the revised payment services directive, aka PSD2, an initiative to create a European digital single market for payment services. PSD2, introduced in January this year, aims to encourage innovation, competition and efficiency in the EU retail payment market, while also tightening the security standards for online payments. It requires banks to share the bank account data of their customers with a wide range of third-party payment service providers.

Also introduced at the start of 2018 was the revamped Markets in Financial Instruments Directive (MiFID II), an extensive piece of legislation to provide greater protection of investors and improve transparency in asset classes ranging from equities to fixed-income, exchange-traded funds and FX.

Ideally, all of this new legislation would dovetail seamlessly. The reality is a degree of conflict; for example, with MiFID's aim of protecting investors through the collection of more information about them and their activities at odds with GDPR's remit of beefing up their data privacy rights. It has been suggested this creates a difficult balancing act for banks and insurers.

At first glance, it may seem that MiFID II, PSD2 and also Open Banking are in conflict with the GDPR, agrees Good. "Elements of all of these regulations cover the need to collect and share information with others – sometimes with the individual themselves, sometimes with other bodies the individual has designated, or with investors," she notes.

"Yes, the GDPR raises the bar in relation to the capture, processing and sharing of personal data, but it does not forbid the disclosure of that data – rather, it sets in place stronger rules for the way in which that can happen. Being wholly transparent, keeping data secure and giving the individual choice and control are key.

"So, rather than creating conflicts, I would say there is an overlap in these regulations in that all require the capture, processing and sharing of personal data, some of which may be sensitive in nature."

A competency test

For corporate treasurers, the GDPR is a further test of the competency of their relationship banks, suggests Joanna Bonnett, group treasurer of PageGroup, a global recruitment business with more than 100 subsidiaries around the world. How competently does the bank handle personal ID submitted to it? And does it spare treasury teams the need to keep asking their senior people for the same ID multiple times?

Do corporate treasurers also need to be aware of the GDPR and its implications? Yes, very much so – as do the organisation's legal and compliance teams, and also the company secretary. All have to be involved with the GDPR and ensure the organisation meets with its requirements. The penalties for non-compliance are severe, with potential fines of up to €20m or 4% of the organisation's global turnover for the most serious breaches.

However, Bonnett believes that treasury departments can't assume their bank will be proactive on the GDPR. "The onus is on us to approach them, as banks are typically internally rather than externally focused," she suggests. "We've ensured that the terms and conditions with each of our banking partners has been updated, which, while it proved to be a lengthy process, was a relatively straightforward one.

"We need to ensure that terms and conditions are updated accordingly and that these updates extend to items such as payroll files, which include a large amount of data." She notes that KYC has already gone from "a cottage industry" 10 years ago to an industrial one – a lengthy and highly complicated process that organisations are obliged to go through every year.

Many organisations will have European directors working in regions of the world such as Latin America, who are covered by the GDPR regulations, although they might be resident in Brazil.

"Too often the Latin America bank providers either haven't heard of the GDPR, or have heard, but aren't bothered about it and haven't done anything to ensure they comply," says Bonnett. "Other jurisdictions, such as Japan and Australia, have their own equivalent of the GDPR, but it may not be the same in all respects."

GDPR and treasury

- The GDPR affects KYC data in two ways. Increased security requirements should spur companies to review internal policies, such as allowing employees to bring their own unsecured devices and allowing them to take sensitive data home at evenings and weekends (at least where that sensitive data may contain personal information). Information security protocols must be defined and upheld in each area of the organisation. It also means the increased use of automation in customer onboarding, monitoring and data-enrichment processes required for meeting the GDPR's requirements.
- Treasurers shouldn't be afraid to ask how their bank addresses the delicate balance of requirements created by recent regulation; for example, the apparent tension between protecting investors under MiFID II through the collection of more information about them and their respective activities, while respecting their strengthened data-privacy rights under the GDPR. What does the bank do with the KYC data submitted? Is it securely stored or destroyed once the details are verified?
- The GDPR's requirements are set out in full by the Information Commissioner's Office. See ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources

Graham Buck is a freelance journalist specialising in treasury, risk management, insurance and pensions