

Are we there yet?

Becoming fully compliant with GDPR will take some companies time to achieve, says **Kieran Kilmartin**, Director of Marketing at **Pitney Bowes**. But it will be worth it in the end...



“Regulatory change is a good thing,” says Kieran Kilmartin emphatically.

As marketing director EMEA for Pitney Bowes, a company that helps power billions of dollars of transactions across borders every day and whose job is made infinitely more complex by new rules, that sounds a little odd, to say the least.

“Compliance and regulation are costs, not money makers,” he adds. Warming to his theme, he adds: “However, better data management is always a plus and can have very positive business effects.

“At Pitney Bowes we look at businesses where there are many customers, large volumes of data, and complex relationships within the data. The upcoming General Data Protection Regulation (GDPR) is an opportunity to improve those relationships and processes across organisations.”

As well as managing data, effective communication is a big part of regulation. Clearly, the GDPR and anti-money laundering (AML) initiatives, which span all industries and geographies, are prime topics at the moment. If you consider AML, it’s about entities, individuals, parties, and ensuring that you can understand the relationships across those different parties, whoever they might be.”

In his opinion, one of the biggest challenges for banks is the ability to track and resolve data issues and because the banks have many disparate systems, criminals exploit any organisational gaps.

He’s hoping GDPR will help to plug them.

“Large retail banks have a vast data challenge. I was talking with a bank the other week, and one of its biggest challenges, given its huge customer base, is to gain consent to process data, and to understand where the customer data is.

“A big difference between the

Data Protection Act and the GDPR is that with GDPR you have to demonstrate that you know what you’re doing. You have to show you’ve got clear processes, and you’re on top of your data. For a lot of organisations, the Data Protection Act was simply about knowing how to avoid fines – minuscule fines compared to those expected with GDPR.”

It will be a huge cultural change for many organisations, he says, not helped by the sheer amount of data collected since the original DPA was enacted in 1998.

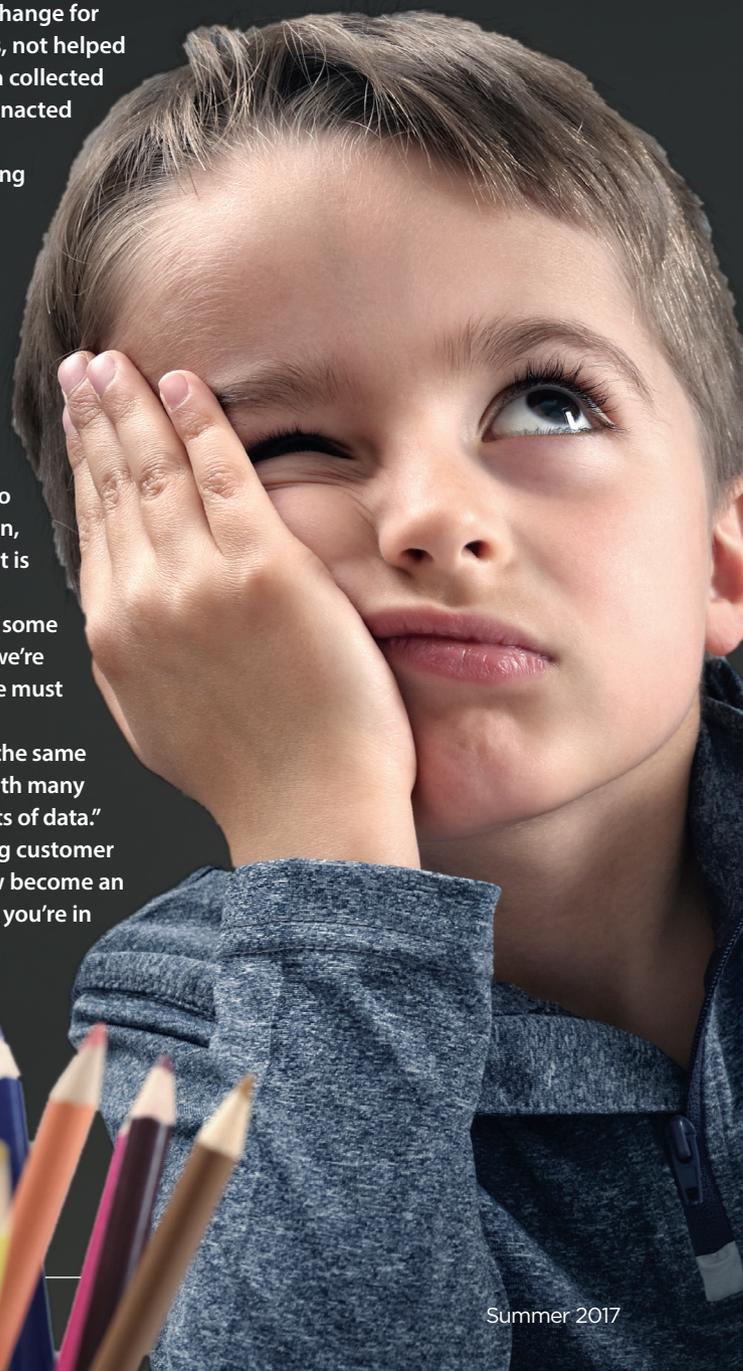
“The amount of data flowing around the internet was minimal compared to today,” he says. “Now, organisations must be far more proactive and attentive, and make people aware of what GDPR means. Within our own business we have documentation that is sent to every part of the organisation, so people understand what it is and what their data responsibilities are. We have some two million customers, and we’re trusted with their data, so we must ensure that our employees understand regulations. It’s the same for any large organisation with many customers and large amounts of data.”

He underlines that gaining customer consent to use data has now become an organisational imperative if you’re in financial services.

“GDPR for banks is all

about profiling data on every party in the value chain and making sure that it’s controlled and compliant. Banks know they have major data management problems and GDPR is a compelling event for them. It’s forcing them to get the house in order.”

So, what are the plusses?



"It's a data solution," says Kilmartin. "Because GDPR and AML provide a single view of the business and the customer, once you're GDPR compliant and have effective measures in place for AML you have the essence of a single view. And the benefit of a single view is that you can provide a better customer service. Although you could say that the return on investment is not being fined, there is also a return in terms of customer service.

"I always think of a single customer view as two sides of the same coin. On one side you have compliance, with people doing what they need to do, but without considering the other side of the coin. The other side is the shiny one, where the marketing and sales functions are, and which is about service."

As well as consent, trust is a fundamental plank of GDPR.

Kilmartin explains: "For many years there's been a lack of trust in banking organisations. We need to share data as well as protect it, which is a problem if trust is missing. Perhaps that appears to fly in the face of GDPR, which is about protecting data, but you need to be confident about sharing data as well as protecting it.

"Pitney Bowes has a long history of helping organisations with data. We have technologies that allow organisations to connect and rationalise data, and that's one of the biggest challenges, because of the disparate and complex data sources in banking. From an AML point of view, there are blind spots, which we help organisations to navigate. For example, when it comes to customer

due diligence, we help organisations make sure that the person they are onboarding is who they say they are.

"As for transactions, banks would rather inconvenience us than risk being fined, so there are many inefficiencies and false positives to root out. We help through automation, ensuring that a transaction doesn't need to be removed from the system for manual intervention. Our strength is to bring data together, without creating an impenetrable data lake. Data is federated across multiple data sources, and draws on the power of our matching engines."

This brings us back to the importance of having a single view.

"Once you've matched the data," says Kilmartin, "you have your single view, whether it's for GDPR or AML. We have a very robust platform, and it's why large banks are using us for AML. We're also talking to tier 1 and tier 2 organisations about GDPR, and how we can help them to find where their data is and why they're holding it."

The importance of that single view becomes very apparent when you consider the number of subject access requests (SARs) from customers demanding to see and vet the information held on them, which are likely to be triggered next year.

"There may be challenges when

someone requests data to be erased, for example," says Kilmartin.

"It's your right to have data erased if it's no longer relevant, but there might be instances where there's a legal, or contractual, reason why it should be kept. This is where we help organisations create a single view very quickly, across multiple data sources. Whether for GDPR or AML, the underlying technology is basically the same."

Although 25 May 2018 is when GDPR comes into effect, Kilmartin suspects many companies will take months to tick all the boxes so they are fully compliant with the regulation and will be made examples of if they fail the deadline.

"My feeling is that a lot of organisations won't have everything in place by next year," he says.

"When the GDPR talks about fines, it says they have to be effective, proportionate and dissuasive. I think the operative word is dissuasive. They'll want organisations to hurt if they don't comply. But the flip side of this is that we will see the vast majority of companies making sure they are compliant or at the least making considerable progress towards it.

"All in all, GDPR is a game changer for all involved."

“ We have technologies that allow organisations to connect and rationalise data – and that's one of the biggest challenges