PaymentsCompliance

Published on *PaymentsCompliance* (https://paymentscompliance.com)

UK Data Watchdog Reassures Financial Firms On PSD2, GDPR Overlap

29TH NOV 2018 | WRITTEN BY: JACOB ATKINS

The UK's data protection regulator has reassured financial institutions that it will work with them to navigate potential clashes between separate EU legislation on payment services and data privacy.

Financial operators have been puzzled at how to reconcile certain aspects of the revised Payment Services Directive (PSD2) and the General Data Protection Regulation (GDPR), both of which took effect within months of each other this year.

There have been attempts to tackle confusion over certain shared language, such as through a European Data Protection Board opinion issued in July, but for some there remains confusion between a directive forcing firms to open access to customer data and a regulation that hands users greater control.

"We don't see that there is a clash there," Richard Syers, a senior policy officer at the Information Commissioner's Office (ICO), told attendees at Payments International on Wednesday.

"The GDPR is very principles-based, it's very context-sensitive, so if you have to do something because the law requires you to do it, generally speaking the GDPR includes the gateway to allow you to do that."

Syers said that the ICO, which is in charge of supervising and enforcing the UK's data protection regime, has worked hand-in-glove on the issue with the Financial Conduct Authority (FCA), which oversees the retail banking and payments sectors.

"We liaise very closely with the FCA to ensure that when they do put requirements in place, or when they interpret laws like PSD2, they are doing so having considered what data protection requirements there are," he told the London audience.

Under the GDPR, national authorities have the power to slug non-compliant organisations with fines of up to €20m or 4 percent of annual turnover.

Enforcing the UK's own Data Protection Act prior to the reforms, the ICO did not shy away from taking aim at some of the biggest names in technology and commerce, including Uber, Facebook, Equifax and even London's Metropolitan Police.

But for payment providers battling with both texts, Syers said that fines would be a "worst-case scenario" if companies could show they had tried hard to comply with both PSD2 and the GDPR.

He said the ICO and FCA "will take a reasonable approach to how we enforce data protection law if you are an organisation trying to comply with lots of different things".

"So if we can see that what you've done is you've tried to comply with PSD2, for example, in a way that's the best you can, and the decisions you've made are based on the considerations of the two, we will take into account the fact you are under those different pressures when we're looking at any issues and we're trying to advise you".

He added that "we'd always want to try to work with organisations first" before getting to the stage of levying fines.

> "If a bank received a verified authenticated request ... under open banking, we are satisfied that the bank has explicit consent for the release of that information to the third-party provider," said Richard Syers of the Information Commissioner's Office.

Providers of payment accounts — typically but not exclusively banks — will become subject to unprecedented data sharing rules once PSD2's regulatory technical standards on security take effect in September 2019.

Some have expressed unease because some transaction data could contain sensitive personal information considered to be a "special category" under GDPR rules. Breaches of such data are in the higher of the two-tier fines system in the regulation's enforcement regime, alongside failures related to personal data, processing and consent.

Payments to political parties, unions, health treatment services or sexual service providers are commonly cited examples. Biometric information is also covered.

However, Syers said that "explicit consent" rules in PSD2, in which customers should be told what data will be collected and how it will be used by a third party, will be enough for the ICO to be satisfied that customers have agreed third-party providers can access "special category" payment data.

"If a bank received a verified authenticated request ... under open banking, we are satisfied that the bank has explicit consent for the release of that information to the third-party provider," he said.

The issue has caused some confusion because GDPR also contains provisions on "explicit consent", but the European Data Protection Board has confirmed the concepts are different under each set of legislation.

Uncertainty around the issue was enough to stall the Netherlands' transposition of PSD2, as the country's data protection body insisted that the boundaries between the payments overhaul and the data protection regulations gave rise to supervisory issues.

This article was amended on November 29, 2018, to clarify that several types of GDPR breaches qualify for a higher-tier fine.

TOPICS

Filter: Data Protection

Filter: Payments Regulation

Consumer Protection

Data Protection

Personal Data

Open Banking

GEOGRAPHY

United Kingdom

Europe

SECTORS

Banking

Fintech

Third-Party Providers

Payment Processing

CONTENT

Insights & Analysis
