FMBusinessDaily

Are You Ready for the Data Protection Changes Coming June 2026?

2 hours ago

From 19 June 2026, two changes to UK data protection law come into force that affect how your organisation handles personal data. Both carry real compliance obligations. Neither has an exemption.

Grant Foster, Partner and Risk Advisory Leader at Howden Risk Advisory said: “From 19 June 2026, UK organisations face two clear, non-negotiable shifts in data protection requirements: a mandatory, formalised complaints process for all data controllers, and significantly higher expectations around transparency when AI is used to process personal data. These changes mark a decisive move by regulators to put accountability and clarity at the centre of data governance, with no exemptions by size or sector and a clear expectation that organisations handle concerns directly before they reach the ICO.

“At the same time, organisations must ensure their privacy notices plainly explain how and why AI is used, what data it touches, and how individuals can challenge or seek human review of decisions that affect them. For many, particularly across financial and professional services, this will require urgent review and updating of existing processes and disclosures, as regulators signal that vague or outdated approaches will no longer meet legal standards.”

The first requires every data controller to have a formal process for handling data protection complaints. The second raises the bar on how clearly you tell people when AI is involved in processing their information. If either of these is not already on your radar, the time to act is now.

A complaints process is no longer optional

Until now, handling data protection complaints well was considered good practice. From 19 June, it becomes a legal requirement under Section 103 of the Data (Use and Access) Act 2025.

The ICO has confirmed there are no exemptions. Every organisation that processes personal data must have a formal complaints process in place, regardless of size or sector.

What does that actually mean? Organisations need to give people a clear way to raise a complaint, whether that is by email, phone, an online form or post. Complaints must be acknowledged within 30 days. Organisations must investigate and respond without unnecessary delay, keep the person informed throughout and tell them the outcome, including their right to escalate to the ICO if they remain unhappy. Their privacy notice must also make clear that individuals can complain directly to them.

One detail worth noting: complaints must be accepted however they come in, including via social media. That has practical implications for how your teams recognise and log them day to day.

The shift here is meaningful. Previously, individuals could go straight to the ICO with a data protection concern. Under the new framework, they are expected to come to you first. That puts the responsibility on organisations to handle complaints properly before they escalate to the regulator.

Telling people about AI is already a legal requirement

The ICO has been clear on this for some time. If AI is being used to process personal data and your privacy notice does not say so clearly, you risk breaching your transparency and accountability obligations under UK GDPR Articles 5(1)(a), 12 to 15 and 22.

The standard expected is not a vague line buried in your terms and conditions. Your privacy notice needs to explain, in plain English, where AI is used and why, what personal data it touches, whether that data is shared with third-party AI platforms and whether it is used to train or improve AI systems. It also needs to cover how AI influences decisions that affect individuals and what someone can do if they want a human to review an outcome.

That last point matters particularly in pensions, insurance and risk advisory. Where AI supports assessments or decisions that have a real impact on clients or scheme members, people have the right to object, request a human review and challenge the result.

The ICO is also explicit about language. Technical jargon and legalistic phrasing do not meet the standard. If a client reads your AI disclosure and cannot understand what it means for them, it needs rewriting.
AI adoption across professional and financial services has accelerated quickly. Privacy notices have not always kept pace. If yours predates the AI tools now embedded in your operations, it almost certainly needs a look.

What organisations should you do now?

Do not wait for the next scheduled review.

On the complaints side, check whether they have a formal process in place. If they do, test it against the new requirements, particularly the 30-day acknowledgement window and whether your privacy notice clearly tells people they can come to the organisation directly. If they do not have a process, build one before 19 June.

On AI, map where AI tools are used across the organisation and what personal data they involve. Read

their privacy notice as if you were a client seeing it for the first time. If it would not make sense to them, rewrite it.

On both, make sure their people know what to do. Staff need to be able to recognise a data protection complaint when it comes in and understand what your AI disclosures actually say.

Why does this matter?

Clients, regulators and counterparties are paying closer attention to how organisations handle personal data. But for FCA regulated firms, there is an additional dimension worth considering.

The FCA's Consumer Duty requires firms to deliver good outcomes for their retail customers, act in good faith and support customers in making informed decisions. Being open and honest about how personal data is used, including where AI is involved, sits directly within those expectations. The FCA's own review of Consumer Duty implementation highlights consumer understanding as a key area, with firms expected to communicate clearly and in a way customers can genuinely act on.

Getting your privacy notices and complaints process right is not just about GDPR compliance. It is also evidence you can point to when demonstrating to the FCA that you are being open and honest with your clients about what you do with their data. The two frameworks reinforce each other, and firms that treat them as separate exercises are making more work for themselves.

The FCA has significant enforcement powers and uses them. Framing data protection improvements as part of your broader Consumer Duty programme is a sensible way to make the case internally and to your regulator.