RR COMPLIANCE associates

Regulatory Update

Volume #9
9 March 2026

REGULATORY UPDATE.

Need Help? Speak to Our Experts!

Book a free consultation and get **tailored compliance solutions** to navigate FCA, ICO or EEA related regulations with ease.

[Book a Free Consultation]

REGUALTORY UPDATES

Stay ahead of regulatory changes with our regulatory updates, expert insights, and industry best practices – just read the update below and share with colleagues.

Download Our Free Desk Aids

We have issued a number of free desk-aid to assist you with understanding, self-assessment and implementation.

- ✅ Download the latest free desk-aid today to evidence compliance

RegZone.io - innovative AML Tool

Stay compliant with automated, real-time checks against global sanctions lists and politically exposed persons (PEPs).

- ✅ Accurate & fast AML screening
- ✅ Reduce costs without compromising compliance
- ✅ User-friendly interface & seamless integration

OFSI investigates first cyber sanctions breaches

26 Feb 2026

Applies to: All firms

Summary

Based on a freedom of information request, OFSI is investigating up to five suspected breaches of the UK cyber sanctions regime. These are the first known live investigations since the regime was introduced and that all of the suspected cases involve financial services firms.

The UK cyber sanctions regime is set out in the Cyber (Sanctions) (EU Exit) Regulations 2020. GOV.UK guidance explains that the regime allows asset freezes and prohibits making funds or economic resources available, directly or indirectly, to designated persons, including entities owned or controlled by them. The guidance also confirms that breaches of the financial sanctions provisions are criminal offences and that relevant firms have reporting obligations where they know or suspect a designated person or a possible breach.

This is particularly relevant in the context of ransomware and complex payment chains. HM Treasury's Financial sanctions guidance for ransomware, published on 28 January 2026, states that making or facilitating a ransomware payment to a designated person can expose a firm to civil or criminal penalties, including where cryptoassets are involved. It also says firms should report suspected breaches to OFSI as soon as practicable.

The practical message is that cyber sanctions enforcement is no longer just theoretical. OFSI's published guidance says the maximum civil monetary penalty is the greater of £1 million or 50% of the value of the breach, and criminal offences can carry up to seven years' imprisonment or a fine, or both. Separately, OFSI has said publicly that it has made significant improvements to its tools, processes and intelligence and will continue to prioritise sanctions enforcement.

ACTION FOR FIRMS

- Boards and senior management should review whether sanctions controls adequately cover cyber incidents, ransomware scenarios, complex payment chains and any cryptoasset exposure.
- Firms should ensure their incident response and escalation procedures require sanctions screening before any payment is made, with clear reporting routes to OFSI.
- Training, record-keeping and third-party oversight should be refreshed so the firm can evidence due diligence and decision-making if OFSI reviews a case.

ASK A QUESTION ->

Further reading ->

Consumer Duty Board Reports – Good and Bad Practice Guide

9 April 2026

Applies to: Principal firms, ARs

SUMMARY

As already reported by us, HM Treasury has launched a consultation on targeted legislative reforms to the Appointed Representatives (AR) regime. The consultation was published on 12 February 2026 and closes on 9 April 2026.

By way of re-cap, the proposals are aimed at tightening oversight and improving consumer protection. The consultation says there are around 34,000 ARs operating under around 2,400 authorised firms, and that poor oversight by some principals has created consumer risk.

The main proposals are:

- a new FCA permission for firms that want to act as principal;
- a targeted extension of FOS jurisdiction, so complaints could in limited cases be considered directly against an AR where the principal is not responsible; and
- bringing ARs within scope of the reformed SM&CR, including applying conduct standards more consistently across principals and ARs.

HM Treasury is also proposing to move detailed requirements on AR contracts and register-related requirements more fully into FCA rules, and to repeal section 39A FSMA on tied agents on the basis that it no longer serves a useful purpose. Existing principals would not need to reapply immediately for the new principal permission, as they are expected to be deemed to have permission, although the FCA could later vary or withdraw that permission.

ACTION FOR FIRMS

- Principals and ARs should start assessing contractual, complaints-handling and accountability implications now
- Boards and senior management of principal firms should review whether their AR governance, oversight resources and MI would stand up to a future FCA permission gateway.

ASK A QUESTION ->

The consultation ->

New data protection complaints handling requirements from June 2026

12 Feb 2026

Applies to: All firms

SUMMARY

The ICO has published guidance on new requirements for organisations to have a process for handling data protection complaints. The guidance was published on 12 February 2026 and says the new requirements are not in force until 19 June 2026, although most of the remaining data protection provisions in the Data (Use and Access) Act framework commenced on 5 February 2026. The ICO also states that there are no exemptions from the requirement to have a complaints process.

The underlying legal change is in section 103 of the Data (Use and Access) Act 2025, which inserts section 164A into the Data Protection Act 2018. This gives data subjects the right to complain directly to the controller where they consider there has been an infringement of the UK GDPR or Part 3 of the DPA 2018. Controllers must facilitate complaints, including by providing a route that can be completed electronically and by other means, acknowledge receipt within 30 days, and without undue delay take appropriate steps to respond and inform the complainant of the outcome. Appropriate steps include making enquiries and keeping the complainant updated on progress.

The ICO's guidance makes clear that firms do not need a separate standalone data protection complaints tool if their existing arrangements can be adapted to meet these obligations. It also says firms must accept complaints however they are received, should make sure staff can recognise and route them correctly, and must tell people that they can complain both to the firm and to the ICO, including in privacy information and when responding to subject access requests.

ACTION FOR FIRMS

- **Boards and senior management should ensure the firm's complaints, privacy notice, SAR and escalation processes are updated before 19 June 2026 so that data protection complaints can be identified, acknowledged within 30 days, investigated without undue delay and evidenced properly.** In practice, firms should also check that existing FCA/DISP complaint routes will capture and route data protection complaints effectively, rather than assuming current arrangements already meet the new statutory requirements.

ASK A QUESTION ->

The ICO Guide –>

RR COMPLIANCE associates

RR Compliance Associates are a trading style of R&R Compliance Consultants Ltd, a limited company registered in England and Wales (company number 12070286). Our registered office is 51 Lime Street, London, EC3M 7DQ.