The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

Dame Chi Onwurah MP
Chair
Science, Innovation and Technology Committee
House of Commons
London
SW1 0AA

Our reference: ICO/O/JE/L/RTL/0808

By email to: commonssitc@parliament.uk

28 July 2025

Dear Chair,

Re: 2022 Ministry of Defence Data Breach

Thank you for your letter of 17 July regarding the details of the 2022 Ministry of Defence (MoD) data breach.

Summary

In your letter you ask that I "confirm that your response to this particular alert conformed with your usual approach to investigating leaks; and usual methods of assessing an organisations' internal handling of data breaches".

The brief answer is, that because of the unusual circumstances of the super injunction, and the classified nature of the information, "No".

However, in substance, our approach to this matter was consistent with our involvement in a great many similar breach notifications in that we indicated areas of inquiry, asked direct questions, and satisfied ourselves that MoD was applying sufficient diligence, rigour and direction to its internal review.

Additional Background

As the Secretary of State said in his statement to Parliament, the ICO was informed within 72 hours of the MoD becoming aware of the breach. This was in August 2023, as the MoD itself did not become aware of the breach until then. The 72-hour notification period in UK data protection law begins when the organisation becomes aware of a personal data breach, as set out in Article 33 of the UK GDPR.

Our response to this breach report was impacted by the circumstances surrounding this case. The court injunction meant we were unable to communicate externally about our involvement until 15 July.

The highly classified nature of the relevant information meant only a very limited number of my staff with the necessary security clearances were involved. We were also limited to oral briefings from the MoD on the details of the case. It was for these reasons that we worked closely with the MoD during its own investigation to assure ourselves that it was taking the necessary steps to address the issues and minimise the risks of them occurring again.

Notwithstanding these circumstances, we did make our enquiries with the MoD as we would for a similar breach of this nature. This included understanding what steps had led to the breach, the causes of the breach and the associated processes the MoD had in place at the time, as well as the steps taken by the MoD to respond to the breach, mitigations for people affected and how it was improving its practices.

Given the understandable commentary and scrutiny around this issue, I have taken the step of publishing more detail about our approach in this case.

Next Steps

I hope the above reassures you and your committee about our approach to this case. We are keeping the situation under review and may choose

to revisit our position if new information comes to light. I stand ready to provide your committee, and any others in Parliament, with the information you need to scrutinise this very serious issue.

Finally, thank you for providing your letter (dated 24 July) to the minister on government data handling. I am including a copy of my letter to the same ministers on the same issue.

Yours sincerely,

John Edwards
UK Information Commissioner

Copied to:

Mr Tanmanjeet Singh Dhesi MP, Chair, Defence Committee

The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

The Rt Hon. Pat McFadden MP,
Chancellor of the Duchy of Lancaster
Cabinet Office
70 Whitehall
London
SW1A 2AS

Our reference: ICO/O/JE/L/ERL/0809
By email to: ministerial.correspondence@cabinetoffice.gov.uk

25 July 2025

Dear Rt Hon. Pat McFadden MP,

Subject: Stopping Data Breaches in Government

I am writing to seek the commitment of government to do more to prevent data breaches in the public sector.

This letter comes in the wake of recent high-profile data breaches in government and the wider public sector, including:

- last week's Ministry of Defence (MoD) disclosure of the Afghan staff data breach;
- a similar breach by the MoD in 2021;
- the PSNI breach which put at risk the lives of serving police officers.

These breaches have real world consequences including putting lives at risk and undermining public trust in government.

My office has made a commitment to try a different approach to regulating the public sector. This approach recognises that monetary penalties often take resource away from vital front-line services and risk re-victimising people relying on those services who have been impacted by a breach.

As part of our public sector approach, both the ICO and government, through a memorandum of understanding with the Permanent Secretaries in the DSIT and the Cabinet Office, have committed to working together to raise standards and ensure we use incidents to learn lessons and prevent future harm.[1]

Some progress has been made, but the government needs to go further and faster to ensure Whitehall, and the wider public sector put their practices in order. As a matter of urgency, the government should fully implement the recommendations of the Information Security Review which the Cabinet Office undertook following the PSNI breach.

A key recommendation of the Review was for the Civil Service Operations Board (or an alternative cross government board) to assume responsibility for establishing a strong senior leadership voice for consistent data protection practice across government, including lessons learned from significant breaches.

Central coordination across government is essential for avoiding further incidents of this seriousness. I would therefore be grateful if you could provide me with an update on whether this and the other recommendations have been implemented.

As you know, I am fully committed to supporting the government in its ambitions to transform the public sector and unleash the power of technological innovation in the economy. This can only be achieved if there is public trust in the ability of government to handle personal information securely; that trust is undermined by breaches of this nature.

I would like to meet with you and your ministerial colleagues as soon as possible to discuss these issues and agree a set of practical actions you will take for improving systems and practices. I will ask my office to liaise yours on a mutually convenient date.

[1] 4 September 2025: the following update has been received from the Information Commissioner's Office: "The Information Commissioner's letter to the Chancellor of the Duchy of Lancaster dated 25 July 2025 about the 2022 MoD breach referenced a memorandum of understanding between the ICO and the Government. For clarification, as set out in our statement at the time, the Information Commissioner received a commitment from Government, specifically DCMS (now DSIT) and Cabinet Office to create a cross-Whitehall senior leadership group to encourage compliance with high data protection standards. However, we acknowledge this was not in the form of a formal MoU and the letter has now been amended for the record".

Finally, the Chair of the Science, Innovation, and Technology Committee has provided me with a copy of her letter (dated 24 July) to you about this case. In the interests of transparency and completeness I will also provide her with a copy of this letter.

I look forward to your response.

Yours sincerely,

John Edwards
UK Information Commissioner

Copied to:

The Rt Hon. Peter Kyle MP, Secretary of State for Science, Innovation and Technology

Sir Chris Wormald KCB, Cabinet Secretary