Capita Data Breach:
Guidance for UNISON branches with affected members

UNISON
the public service union

5 September 2023

Capita Data Breach: Guidance for UNISON branches with affected members

This is the latest update for UNISON EA and NRW members that are members of the EAPF have been affected by the recent hacking attacks on the outsourcing firm Capita.

We are aware that members have told us they are experiencing fear, anxiety and stress because of privacy violations and are wanting to understand what legal avenues could be available because of this breach. There will be tens of thousands of individuals affected by this incident.

The breach affects:

1. Members of the EAPF that have retired and are already in receipt of their pension
2. Members working for the EA that are members of EAPF but have not yet retired
3. Members who are no longer working for the Environment Agency that have not yet accessed their pension.

If you or a family member also affected by the breach are experiencing tress or anxiety because of this data breach please contact your local branch health and safety representative. They will be able to provide advice in relation to logging this on Airsweb.

In addition, please contact your UNISON EA branch if you can identify a fraud that has taken place in your name that can be attributed to this data breach.

Background

Capita administers around 450 pension schemes in the public and private sectors.

According to the Information Commissioner's Office, around 90 organisations have reported data protection violations related to this incident.

Capita provides outsourced pension administration services to over 450 pension providers across the UK. Several of them have confirmed that they are affected by this breach.

The first data breach relates to a ransomware cyberattack that happened 31 March 2023. It is understood that this originated from a 'phishing email that contained a malicious weblink'. This enabled criminals to exfiltrate / copy data from Capita's shared network folders , where personal data was being stored about members receiving their pension.

Importantly the data is not 'missing' – it was copied. and the Pension Payment System remained secure.

The EA has provided a full list of personal data believed to have been stored that may have been accessed by hackers.

The data breach occurred in late March 2023, and it appears that the EA was initially notified in mid-May 2023 of a partial data breach and reported the breach to the Information Commissioner's Office (ICO).

The delays in notifying employers is something regulators will be investigating. Further details were released in early July 2023 as an internal audit carried out by Capita established the breach was significantly greater than initially understood.

Who is responsible for securing my personal data?

Your employer, the Environment Agency is a 'data controller'. As a data controller, they are responsible for ensuring **any data processing – including any data processing carried out by a contractor data processing on your behalf** – complies with the UK GDPR.

UK GDPR responsibilities include the following:

- **Compliance with the data protection principles**: Data controllers must comply with the data protection principles listed in Article 5 of the UK GDPR.
- **Individuals' rights**: Data controllers must ensure that individuals can exercise their rights regarding their personal data, including the rights of access, rectification, erasure, restriction, data portability, objection and those related to automated decision-making.
- **Security**: Data controllers must implement appropriate technical and organisational security measures to ensure the security of personal data.
- **Choosing an appropriate processor**: Data controllers can only use a processor that provides sufficient guarantees that they will implement appropriate technical and organisational measures to ensure their processing meets UK GDPR requirements. This means the EA is responsible for assessing that any contracted data processor is competent to process the personal data in line with the UK GDPR's requirements. This assessment should consider the nature of the processing and the risks to the data subjects.
- **Processor contracts**: Data controllers must enter into a binding contract or other legal act with your processors, which must contain a number of compulsory provisions as specified in Article 28(3).
- **Notification of personal data breaches**: Data controllers are responsible for notifying personal data breaches to the ICO and, where necessary, other supervisory authorities in the EU, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Data controllers are also responsible for notifying affected individuals (if the breach is likely to result in a high risk to their rights and freedoms).
- **Accountability and governance obligations**: Data controllers must comply with the UK GDPR accountability obligations, such as maintaining records, carrying out data protection impact assessments and appointing a data protection officer.
- **International transfers**: Data controllers must comply with the UK GDPR's restrictions on transfers of personal data outside of the UK.
- **Co-operation with supervisory authorities**: Data controllers must cooperate with supervisory authorities (such as the ICO) and help them perform their duties.

The ICO information for data controllers can be found here: ICO what does it mean if you are a data controller

Can data controllers be held liable for non-compliance?

Yes. Data Controllers are ultimately accountable for compliance and the compliance of any contracted data processors. An individual can also bring claims directly against a data controller if the processing breaches the UK GDPR, in particular if the processing causes the individual damage.

However, data controllers are not liable for damage resulting from a breach of the UK GDPR if it can be proven they were not in any way responsible for the event giving rise to the damage.

UNISON met with the Pensions Regulator 31 July 2023 and raised several concerns in relation to this issue. However, all parties are now awaiting the outcome of the ICO investigation which will establish the facts and determine whether there is any liability.

Our current understanding is that the breach also affects schemes/funds including:

Universities Superannuation Scheme (USS), Diageo, Unilever, Rothesay, Marks & Spencer, PwC pension scheme, BAE Systems, Capita

While Capita's data system was breached - pension schemes are responsible for the security of member data. The Pensions Regulator confirmed this in a statement to trustees of affected pension schemes. Following the breach, both the Pension Regulator and the ICO will likely want to know more about the affected pensions' security measures, and their relationship with Capita in regards to data protection.

UNISON and Prospect has members on the EA Pension Committee and they will also be seeking answers to matters as they are raised, in addition to pressing for a review of the security of personal data moving forward. We will keep branches and members informed of any progress made.

Trade unions have elected representatives to the EAPF Pensions Committee . We will ensure that all relevant information on the data breach is cascaded on the ongoing situation as it becomes available.

UNISON has written to the EA seeking a better understanding of the measures it had in place in relation to personal data storage provided by Capita and continues to meet with the EA to raise matters of concern with the EA.

If you have any queries please raise them with your branch who will escalate this issue on your behalf.

UNISON is pressing for action from Capita, the pension funds, and the Pensions Regulator to mitigate against the risks to members and have called for an investigation into the causes and risks of the leak by the Information Commissioner's Office (ICO).

The ongoing situation remains fluid and further investigations are ongoing. UNISON has pressed this matter with the EA and attended meetings in August 2023 attended by the Pension Fund Manager as well as other senior EA managers.

UNISON has already taken the following actions:

1. The EA has advised they became aware of the issue from Capita initially 19 May 2023 and notified the Information Commissioner's Office (ICO) of the data breach on Monday 22 May 2023.
2. A meeting was held 13 July 2023 where a representative from Capita was in attendance. We fed back concerns raised with the response from Capita in terms of understanding the anger and anxiety of the matter on EA staff.
3. The EA is also liaising collectively with other affected employer pension schemes in approaches to Capita on this matter.

4. The EA has provided UNISON with a copy of the template letter used to notify EA staff of the impacts – and a full set of the list of data that has been breached.
5. UNISON and the EA are exploring whether the data breached was held in accordance with GDPR.
6. UNISON raised the issue of potential impacts for those identified as beneficiaries and those identified as spouse in relation to their data and we will update you when we have a response from EA and / or Capita on this point.
7. The EA and other employers are seeking detailed understanding from Capita. This is subject of an investigation by the Information Commissioner's Office (ICO).
8. UNISON has pressed for clarification on the current level of security of the data that was breached, whether Capita were complying with their contractual obligations and details of what measures are now in place to ensure this data is appropriately encrypted another to prevent a further breach.
9. UNISON requested the risks to members of staff that deal with serious crime are assessed in the H&S risk assessment. Staff that work in this area got to significant lengths to secure their personal information. We are raising with EA what systems are in place to support retired staff in similar circumstances.
10. The EA has produced an FAQ document that is available via Easinet and this will be regularly updated. UNISON will ensure we regularly update members on this matter and will be organising a webinar for members.
11. The EA has agreed to future engagement on this issue to be able to exchange information and provide ongoing support to members.
12. UNISON has requested the EA presses Capita to provide access to CIFAS to provide some protection to identify potentially fraudulent activity at no cost to individuals or the EA. UNISON is pressing the ICO to consider the level of fraud protection that is needed moving forward as individuals have a major 'digital' footprint and breaches of this nature can have a significant impact.
13. The joint trade unions have also asked the EA what actions it will take in terms of reviewing the contract for the administration of pensions and explore alternative options moving forward that provided enhanced data security.

ICO advice re: Identity theft.

The ICO regards that just name, address and date of birth can be sufficient data for a fraudster to attempt identify theft and seek to access loans, state benefits, or make purchases.

We would encourage members to take up the initial offer of Experian identity protection services where offered by Capita or their pension fund in the first instance. UNISON urged employers affected by the breach to put in place enhanced protection – and this has been increased from 12 months to 24 Months at no cost to individuals.

Some members have said that they have concerns in registering for this service. If you need any further information on what the service is and what it offers please contact your local branch who can provide additional details.

Accessing your pension directly. The Pensions Regulator has already instructed schemes to monitor unusual or increased transfer requests. There are no reports of pensions being attacked directly, but we should remain vigilant. Members should be encouraged to remain members of their employer pensions scheme.

Pension scams. The more likely danger to members' pensions is that the leaked data could enable a fraudster to contact them and to speak convincingly such that the member agrees to transfer money to them. Such contact might not be made immediately, but months after the leak.

Members affected by the data breach should not disclose further information and should always request that people who contact them confirm their identity.

Some common signs of a pension scam are:

- Cold calling about a pension – **note that this is illegal**
- phrases like 'pension liberation', 'loan', 'loophole', 'savings advance', 'one-off investment', 'cashback'
- guarantees they can get better returns on pension savings
- high pressure sales tactics – time limited offers to get the best deal; using couriers to send documents, who wait until they're signed

More information on identifying potential scams is available on The Pensions Regulator website.

For any further queries on matters not captured in this briefing please email pensionsqueriesformembers@unison.co.uk

Legal advice

Many members have contacted UNISON in relation to any potential legal action that can be taken in relation to this matter.

At this point in time the ICO is still investigating the issue. We will have more clarity once the ICO has published its findings following its investigation.

There may be potential causes of action against either Capita or the employer. With data protection claims, generally speaking the UK Courts have taken a very stringent approach. This has restricted the ability to succeed in individual cases, and also severely impacted on the ability to take collective action.

The fact a breach has occurred does not automatically give rise to an individual claim in compensation. A potential case could focus on whether the defendant's measures in place to prevent the breach were appropriate. If not, and if the claimant can then show actual damage/harm, of a material (i.e. financial) and/or non-material (i.e. injury) kind, flowed from this breach, a claim may be possible. However, from the UK Courts approach to date, it is also clear, such non material loss must be more than upset, covering for example actual psychological injury – such as distress/anxiety. Each case will turn on its own facts. Once the ICO has published its findings UNISON will provide further information.