information commissioner

Barrantagh Fysseree

Case Study

Case Study: Reprimand issued to Payroll Partners Limited (PPL)

Who?

Payroll Partners Limited (PPL) – a payroll administration company operating on the Isle of Man - experienced a significant loss of control of personal data following the closure of its local operations in March 2024 after a merger.

What Happened?

In August 2024, PPL's former landlord reported to the IOM ICO that two full, unlocked shredding bins containing personal payroll documents had been found in the company's vacated office.

Given the reported amount and sensitivity of the data, the ICO decided to secure the documents while tracking down representatives of PPL.

The ICO collected the documents and transferred them into 14 storage boxes.

'Dip sampling' of five boxes revealed over 9,700 records containing both personal and special category data, including names, salary information, dates of birth, immigration documents, financial records, identification documents, photographs, maternity and sick notes, and more. Records ranged from 2006 to 2024.

In many instances, the personal data combined provided a comprehensive overview of a person, including name, address, dates of birth, and salary information.

In the process of assessing the documents, the Information Commissioner's own personal data (from 2006 rental payments) was found, prompting her to recuse herself. The Assistant Commissioner assumed lead responsibility of the investigation.

PPL were cooperative with the ICO during the investigation.

The Investigation

Once they were made aware of the shredding bins, PPL attempted to retrieve them through local personal contacts. When this was unsuccessful, they did not take further formal legal procedures to retrieve the data.

Despite learning that the shredding bins had not been disposed of as expected, PPL did not recognise the situation as a personal data breach, did not report it to the ICO, and did not assess whether affected individuals should be notified.

The incident highlighted several underlying issues:

- The business shutdown was not managed properly.
- The company didn’t have good enough controls in place to make sure paper records were destroyed safely.
- They didn’t understand when or how to report a data breach, and a lack of accountability.
- Leaving the bins behind showed that the company failed to follow basic data protection rules, especially for handling sensitive personal information.

While the risk to individuals was ultimately assessed as low - largely because the premises were locked - this mitigation arose from circumstance rather than design. Once the ICO secured the documents, any further risk was removed.

Lessons Learned

The case reinforces that organisations remain responsible for personal data throughout the entire lifecycle of their operations, including after closure.

Clear destruction processes are essential. Holding vast amounts of data going back to 2006 shows a lack of retention policy. ICO advice is to only hold on to data that you need.

It can seem like an easy option on a small island to rely on informal contacts or favours but this cannot replace documented, compliant procedures - especially for businesses handling large volumes of sensitive information.