Second accidental data leak in four months ‘regrettable’, finance department says

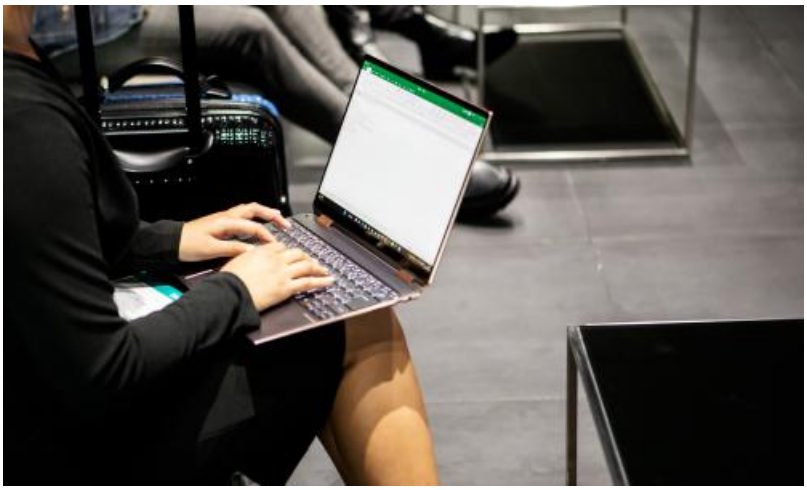
Publication Date: 2024-02-22

Author: Tory Shepherd

Section: Technology

Tags: Data protection, Privacy, news

Article URL: https://www.theguardian.com/technology/2024/feb/22/second-accidental-sharing-of-confidential-information-regrettable-finance-department-says



The finance department has accidentally shared confidential commercial information for the second time as new data reveals the number of human errors behind government data breaches. The department has confirmed that last week it emailed 236 suppliers, and that the email included “embedded information with some third-party confidential information”. The shadow finance minister, Jane Hume, said the breach would damage confidence in the procurement process, especially coming after a similar breach in November last year. “Companies and individuals impacted by this gross incompetence may exercise their rights against the commonwealth, potentially costing taxpayers millions,” she said. On Thursday, the Office of the Australian Information Commissioner released the latest data breach statistics, showing the federal government is back in the top five sectors hit by breaches for the first time in three years. The data shows the government takes longer to identify and respond to breaches than other sectors, and that while usually criminal acts are behind breaches, in government agencies it is more likely to be human error. The finance department said in its statement it has tried to call all suppliers to ask them to delete the email and attachments. It said “no third-party confidential information would have been accessed or viewed by a person who simply opened the email or its attachments”. Sign up for Guardian Australia’s free morning and afternoon email newsletters for your daily news roundup The finance department secretary, Jenny Wilkinson, has directed there be an independent review of that breach and the November 2023 release. It will be conducted by the former commonwealth ombudsman Michael Manthorpe. “The review will consider the circumstances that led to the unauthorised disclosure of the information, as well as the department’s systems and processes,” the department said in a statement. “The potential disclosure of this third-party confidential information is regrettable, and finance apologises for the oversight.” In November 2023, a department officer uploaded confidential pricing information from hundreds of firms to the wrong place within AusTender. The information was then sent out as part of a request for quotes from government departments, making it potentially available to 22 service providers. The providers were then asked to guarantee confidentiality and monitored to ensure they had not used the information to gain a commercial advantage. In the latest breach, the Australian reported that supplier and service provider names and price scales for major firms including Deloitte, KPMG, Minter Ellison and Boston Consulting Group were included on a hidden tab on a spreadsheet. David Pocock, a independent senator for the ACT, said the “repeated and even worse failure of process from the Department of Finance is deeply concerning”. He said it was “very damaging for smaller firms who are now at a serious disadvantage with 236 suppliers having received their pricing details”. “The government needs to immediately spell out what additional steps it is putting in place to ensure this mistake isn’t made a

third time and get on with the serious procurement reform that is long overdue.” According to the OAIC data, health sector providers had the most breaches in the six months to December 2023, with 104. The finance sector was next with 49, followed by insurance (45), retail (39) and government (38). Overall two-thirds of the data breaches were from malicious or criminal attacks including cybersecurity incidents, just under a third were from human error (with information being sent to the wrong person the most common error), while 3% were from a system fault. But that trend was reversed in the government, where 12 breaches were malicious or criminal and 26 were from human error. The government also took longer to identify breaches, with 37% of breaches identified within 10 days, compared with 75% for health service providers. And it took longer to report breaches, with 45% reported within 30 days, compared with 86% for the health sector. “These statistics suggest Australian government agencies should check they have effective systems for detecting, assessing, responding to and notifying data breaches,” the OAIC said. “Such systems are fundamental to an agency’s ability to meet the NDB (notifiable data breaches) scheme’s requirements.”