

OpenVoiceNews Australia

Transparent. Unbiased. Yours.

Data Hack Ignites Push for Political Party Accountability

July 26, 2025

— Categories: *Politics & Government*



On 23 June 2025, political groups linked to businessman Clive Palmer, Trumpet of Patriots and the deregistered United Australia Party (UAP), were targeted in a ransomware attack that exposed sensitive personal data. The compromised information is believed to include email addresses, phone numbers, financial details, and employment records. The organisations publicly confirmed the breach, urging supporters to assume all shared data may have been accessed.

Australia's Privacy Act 1988 currently exempts political parties from mandatory data breach reporting, unlike businesses and government agencies. This legal loophole allowed the incident to remain undisclosed until voluntarily acknowledged. However,

because UAP lost its registered status in 2022, questions have arisen about whether the exemption still applies in this case, raising potential regulatory implications.

Privacy advocates and legal experts have long warned that political parties should not be above the law when it comes to protecting sensitive information. The incident has intensified criticism of the existing exemption, which was originally intended to safeguard political communication but now risks undermining public trust. With political groups accessing electoral roll data and detailed voter profiling systems, the lack of regulatory oversight has sparked renewed demands for reform.

In the wake of this breach, calls are growing for political organisations to be held to the same privacy and cybersecurity standards as other sectors. The government faces mounting pressure to legislate changes ensuring accountability, especially as cyber threats continue to escalate. The incident underscores the urgent need for modernised privacy protections that apply universally, regardless of political affiliation.