Australian Government
Office of the Australian Information Commissioner

OSP arrangements assessment

Summary

In October 2024, the Office of the Australian Information Commissioner (OAIC) assessed the Consumer Data Right (CDR) outsourced service provider (OSP) arrangements of 2 accredited data recipients (ADRs), in their role as OSP principals. We aimed to ensure that the OSP principals had appropriate CDR outsourcing arrangements in place to manage and protect their clients' CDR data. This was a risk and compliance-based assessment.

Our findings

Overall, we found that both OSP principals had taken steps to establish policies, processes and procedures to implement their CDR outsourcing arrangements, each of which generally included the conditions required by the CDR rules. Areas for improvement were identified requiring OSP arrangements to both address legislative requirements and provide compliance monitoring and incident reporting details. Positively, both OSP principals had implemented robust governance structures to ensure they thoroughly vet prospective OSPs' information security capabilities however

Recommendations

We made 6 recommendations and 3 best practice suggestions for one OSP principal, and 3 best practice suggestions for the other. Notably, we recommended that one OSP principal add an indirect OSP to its CDR policy to comply with CDR legislation. We also recommended the OSP add a provision to an OSP arrangement requiring its OSP to comply with relevant CDR service data privacy obligations as if it were the OSP principal. We focused other key recommendations on encouraging the OSP principals to enhance their practices to support the CDR outsourcing arrangements meeting legislative requirements through OSP training, compliance monitoring and incident reporting.

Takeaways

OSP principals must ensure their OSP arrangements address legislative requirements and provide sufficient detail that both parties (OSPs and principals) will find practically informative and useful. OSP principals should tailor OSP arrangements to be relevant to the types of CDR data managed and establish appropriate controls to secure the CDR data that the OSP collects, uses or discloses. OSPs principals should also ensure their OSPs apply the principal's standards in handling CDR data.