Commissioner brief: OAIC regulation of privacy matters relating to offshore contracts

Key points

- Under the *Privacy Act 1988* (Privacy Act), DIBP (now Home Affairs) has a number of privacy obligations in regard to its contracted service providers (**CSPs**).
- In 2016, the OAIC assessed DIBP's contract management in relation to privacy matters for the CSPs operating at its regional processing centres (**RPCs**). Specifically, whether DIBP met its obligations under APP 1.2 (Open and transparent management of personal information) and APP 11 (Security of personal information), and s 95B of the Privacy Act.
- At that time, the OAIC found that DIBP did not have in place adequate formal policies for engaging DIBP's privacy staff and that contractual terms did not adequately safeguard personal information that may be held by the CSPs.
- The OAIC recommended that DIBP include additional provisions relating to privacy and information security in its contracts for services in its RPCs, its contracts for services in its RPCs should include specific categories for reporting privacy and information security complaints and breaches, and that it establish a program of audits to assure itself that its CSPs are meeting their obligations with regard to privacy and information security.
- The OAIC made four recommendations, and DIBP accepted these recommendations.

Application of Privacy Act to DIBP's offshore contractors

- In addition to its requirements under APP 1.2 and 11.1 (with regard to CSPs), s 95B of the Privacy Act requires DIBP to take contractual measures, in any Commonwealth contract that it enters into, to ensure that a CSP does not do an act or engage in a practice that would breach an APP if done or engaged in by DIBP. DIBP must also ensure that its Commonwealth contracts do not authorise a CSP to do or engage in such an act or practice, and to ensure that such an act or practice is not authorised by a subcontract.
- These requirements are related to the APPs —for instance, the reasonable steps to secure personal information, as required under APP 11, may include the use of appropriate contractual measures.

DIBP assessment: 'Assessment of contractual provisions for services in regional processing centre'

- In September 2016, the OAIC assessed DIBP's privacy obligations in relation to its contracts with CSPs for services related to DIBP's RPCs on Manus Island and Nauru.
- Specifically, the assessment considered whether DIBP was meeting its privacy obligations under APP 1.2 and APP 11.

- As the focus of the assessment was on DIBP's contracts for services related to its RPCs, the OAIC also had regard to DIBP's obligations under s 95B of the Privacy Act.
- The scope of the assessment did not consider broader procurement and contract management issues in relation to these RPCs. The OAIC is aware that these matters were considered by concurrent audits of the Nauru and Manus Island RPCs by the Australian National Audit Office.
- The OAIC published this report in March 2018 (https://www.oaic.gov.au/privacy-law/assessments/assessment-of-contractual-provisions-for-services-in-regional-processing-centres-department-of-immigration-and-border-protection).
- The OAIC made four recommendations, and DIBP accepted these recommendations.
- The recommendations, DIBP's responses, and DIBP's actions as of March 2018 are set out in the table below. **A follow-up of this assessment has not been undertaken**.

Document history

Updated by	Reason	Approved by	Date
Kellie Fonseca			

Recommendations

No.	OAIC Recommendation	DIBP Response/ further information	DIBP Action taken
1	DIBP should **ensure that its internal policies and procedures** require that the Privacy and Reviews Section be: ○ consulted during the development of new contracts for services relating to regional processing centres, and ○ advised of suspected or actual privacy or information security breaches and privacy complaints in its RPCs when these breaches or complaints are reported to it by CSPs.	**Agree.** DIBP agrees that consultation with the Privacy Section (formerly Privacy and Reviews Section) should be improved in the development of new contracts. **Agree.** Under the Garrison and Welfare Contract, the CSP must report when suspected Code of Conduct breaches occur at the time of the event, and report monthly on actual breaches. In addition, any suspected privacy or information security breaches are reported through situation reports and investigated by the contract management team.	There are currently a number of contracts being negotiated and the Privacy Section is actively being consulted as part of the process. During end of contract transition, DIBP engages ICT resources to ensure that all systems and data is protected and sanitised. All hard copy records are similarly managed. Any suspected privacy breaches are reported immediately to privacy, IT security and records management teams.
2	DIBP should **ensure that future contracts**: ○ provide guidance to CSPs as to the reasonable steps that CSPs should take to secure personal information. This could include (but should not be limited to) a security standard that CSPs should meet. ○ include provisions ensuring that subcontractors handle personal information in a manner consistent with DIBP's privacy and information security obligations. ○ include provisions setting out CSPs' obligations concerning privacy and information security at the completion or termination of the contract. This should include, as appropriate, destruction and de-identification of personal information, in accordance with APP 11.2 and the *Archives Act 1983* (Cth).	**Agree**. DIBP agrees to consider the scope of guidance and requirements in future contracts with CSPs in relation to securing personal information. **Agree**. Irrespective of the issues that OAIC has noted in the documentation provided to the OAIC for the assessment, DIBP confirms that future contracts require subcontractors to handle personal information in a manner consistent with DIBP's privacy and information security obligations. **Agree**. DIBP agrees to consider the obligations and requirements for each CSP in relation to information security at the completion or termination of the respective contracts.	Privacy and the Records Management Sections have been involved in the current transition/end of contract processes. In addition, oversight by the National Archives of Australia to ensure that all Commonwealth material and privacy considerations are managed. DIBP has in place processes to manage the electronic and paper records/data as part of transition including destruction on authority of the National Records Manager.
3	DIBP's **incident management arrangements** under contracts for services relating to regional processing centres should include an incident category for privacy, including privacy complaints and actual or suspect privacy or information security breaches.	**Agree**.	For future contracts established by DIBP for services that relate to regional processing operations, DIBP agrees to include in the incident management arrangements, protocols or procedures privacy

			concerns, including privacy complaints and actual or suspected privacy or information security breaches. Of particular relevance to existing contracts, DIBP considers that, it and CSPs are able to effectively and expediently address privacy and information security risks by amendments to operational material and relate to the respective contracts — including standard operating procedures, transition plans, etc.
4	DIBP should: ○ **establish a program of proactive privacy** and **information security assurance activities** of CSP's arrangements relating to privacy and information security in RPCs. These activities could include, for example, regular audits or inspections of CSPs' procedures and systems in its RPCs to assure DIBP that privacy and security requirements are being met ○ **ensure that the Privacy and Reviews Section is involved in planning** these activities, and advised of their findings.	**Agree**. **Agree**. DIBP agrees that the Privacy Section should be involved from the outset in planning assurance activities.	DIBP will establish a program of proactive privacy and information security assurance activities of CSPs' arrangements in RPCs. Compliance audits will be undertaken to ensure that CSPs' procedures and systems align with privacy and security approaches. During the transition of contracts, data and information activities are planned with the Privacy and the Records Management Sections in collaboration with IT security to ensure that data and records are protected.