Issued: March2021

Key Privacy obligations for DCJ Contractors

The Department of Communities and Justice (DCJ) works with a number of private sector organisations, Non-Government Organisations (NGOs) and other public sector agencies to deliver services and programs to the NSW community.

Entering into a contract with the DCJ raises important privacy considerations for you and your staff in relation to the collection, storage, use, disclosure and destruction of personal information under the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act).

Privacy Training

It is essential that your staff are trained in their **privacy obligations** on a regular basis, and **before** they are given access to DCJ information. It is a good idea to retain a record of completed training to demonstrate compliance.

Information handling and security

Information collected by you and your staff in the delivery of services and programs is held by you on behalf of DCJ.

The personal information collected by you, must be collected lawfully and where possible directly from the individual. Personal information that is not relevant to the delivery of your service or program must not be collected, such as for advertising, marketing or research purposes.

The information you collect can however be used for program or service analysis and internal reporting.

Your staff should be aware of and familiar with relevant DCJ standards and guidelines. Ask for a copy of the below policies if you do not have access:

- IT Acceptable Use Policy
- Information Security Policy
- Data Breach Response Plan
- Data Privacy and Protection Policy

Personal or health information must not be uploaded or stored on personal devices or IT systems that have not been approved for use by DCJ.

Report data breaches

A data breach or allegation of a breach, which includes the inadvertent or malicious loss, disclosure or corruption of DCJ information, **must immediately** be notified to DCJ.

If a data breach occurs, you and your staff will be required to work with DCJ to:

- investigate the nature and extent of the breach;
- assess the risks and consequences associated with the breach;
- notify relevant regulators (NSW Information and Privacy Commission, the Office of the Australian Information Commissioner, Cyber Security NSW); and
- review the circumstances of the breach and participate in action to mitigate the risk of any future breach.

In addition, any complaints received in relation to a data breach/breach of privacy must be handled in accordance with the PPIP Act / HRIP Act. This will require you to conduct an audit or investigate the circumstances that gave rise to the breach promptly.

Data Retention

Certain obligations under DCJ's contracts extend beyond the term of the contract. For example, Government record keeping requirements may require you to hold information for longer than the period of the contract.

Seek your own legal advice to ensure you comply with the *State Records Act 1998* and any relevant disposal authorities.

Right of access

DCJ has an immediate right of access to the following information:

- Information that relates directly to the performance of the services provided by the DCJ
- Information collected by you from members of the public where you provide, or offer to provide services
- Information received by you from DCJ to enable you to provide services in accordance with your contract

DCJ's immediate right of access is required to meet our legislative obligations under the *Government Information (Public Access) Act 2009* (GIPA Act) and is often in your contract of engagement.

Do you need help or require more information?

Further information about your compliance obligations under the GIPA Act, PPIP Act or the HRIP Act is available through the website of the Information and Privacy Commission.