Privacy Guidelines

FAQ's

November 2020

Why is the Ministry issuing these guidelines now?

It is critical that people's information is treated sensitively, and the Ministry of Justice wants to support third-party providers who deliver services for the Ministry to do this well. The guidelines set clear expectations for how providers should handle and protect the information they hold on the Ministry's behalf.

Most providers already have sensible and effective systems and processes in place to manage sensitive information. Unfortunately, in recent years a range of government agencies have experienced privacy breaches by their service providers. In these cases, harm and unnecessary media attention could have been avoided if basic privacy procedures were followed.

How has the Privacy Act changed?

The Government has recently strengthened the Privacy Act. It is important that both the Ministry and providers are ready for the changes coming into force on 1 December 2020.

The key changes are:

- the requirement for any privacy breaches which pose a risk of serious harm to people to be reported to the Privacy Commissioner and the affected individuals
- new criminal offences: the introduction of fines for both organisations and individuals
- new powers for the Privacy Commissioner to issue compliance orders following any privacy or security breach.

You can read more about these the changes and when they come into effect here: https://privacy.org.nz/privacy-act-2020/resources/

The guidelines the Ministry has developed will help providers understand the new requirements and to put into daily practice concepts such as the 'Principles of the Privacy Act'.

Who do these Guidelines apply to?

The Privacy Act applies to all organisations and the guidelines are a helpful resource for anyone that delivers services to the Ministry of Justice and courts.

Complying with these guidelines will become a requirement for providers that have contracts to deliver on-going services on behalf of the Ministry. Organisations that deliver services such as:

- Family violence programmes
- Restorative Justice
- Parenting through separation
- Community legal services etc

will have an additional privacy clause added to their contracts from 1 July 2021.

The guidelines are being provided as a useful resource to support best practice to Legal Aid Lawyers and providers that deliver one-off or irregular services directly to the courts.

We recognise that lawyers are already subject to professional obligations that go above and beyond the requirements of the Privacy Act, and the legal aid contract has recently been updated to include new privacy clauses.

If your organisation has a Ministry Relationship Manager from Provider and Community Services, they will be in contact with you to discuss how you implement the requirements outlined in the guidelines.

How do I complete the IT Self-assessment?

As much of the information we collect, use and store involves electronic systems, we have included an IT self-assessment to help you better understand if your systems are fit for purpose.

We expect that organisations use this self-assessment and develop plans to address any gaps that are discovered.

We understand that organisations will be at different stages and the cost of upgrading systems can be prohibitive. At this stage the Ministry does not require that all the recommended controls are in place, but we do expect organisations to take their responsibility to protect people's information seriously.

Not all aspects of the IT self-assessment will apply to every organisation, we have separated the controls into two levels with many of the controls in the second level being appropriate for larger organisations.

What if I use sub-contractors to deliver services?

Providers need to take all reasonable steps to ensure any contracted staff manage information appropriately and in compliance with the Privacy Act and the Ministry's expectations. The guidelines will help you do this. For example, good practice looks like:

- contractors meet the same requirements as staff members in regard to training and Police and criminal record checks
- providers control the email accounts information is shared through, and sensitive information is not sent or received from contractors' personal email accounts (this applies to staff too).

In terms of IT, there is a key question in the IT self-assessment that asks if providers control all devices (such as laptops) that store or access sensitive information. While we expect providers to control all devices they use, we realise this may not be the case currently. If a provider cannot provide a device to contractors they should record this, and any other steps they are taking to mitigate risk, on the self-assessment form.

What happens when things go wrong?

We expect providers to have plans and policies in place to prevent privacy and security breaches and manage them if something happens and a breach occurs. If a breach does happen, you must notify the Ministry right away and we will work together with you to ensure the response to the breach is appropriate and fair.

Where breaches have occurred in the past the Ministry has worked with organisations to reduce the impact of the breach and improve processes to prevent further breaches. Cancelling a contract would only be the last resort.

How do the guidelines align with expectations of other government agencies?

There is a lot of information available around privacy and data protection, for example, through the Office of the Privacy Commissioner, Social Investment Agency (SIA) and CERT. The Ministry guidelines align with these resources. We have summarised the key requirements, so it is clear for providers what the Ministry expects from them.

Other funders may, or may not, require providers to comply with the IT controls we have identified as priorities for us. Social Services Accreditation (SSA) will also require the providers they accredit to have basic IT security mechanisms in place.

How will my Social Sector Accreditation be affected?

Social Sector Accreditation (SSA) has reviewed how accreditation assessments accommodate provider privacy requirements in line with the new Privacy Act.

The guidance for the Social Sector Accreditation *Governance and management structure and systems* standard (criterion 6) has been updated. This is to strengthen providers' basic privacy and information security procedures.

The revised SSA requirements also reflect the Ministry expectations.

In terms of IT controls, SSA assessors will require providers to demonstrate that they have fundamental, basic controls in place. You may find it useful to talk through your completed data security self-assessment with any SSA assessor that visits you. This will help them understand how you are complying with their expectations around data security.

Will the Ministry be offering additional support to providers?

We realise providers will be affected differently by the implementation of the guidelines. Therefore, we intend to work closely with providers over the next six months to ensure the guidelines are meaningful and the expectations set are achievable.

While most providers already have the key mechanisms in place there will be some that don't. We do not intend for providers to have to incur major costs or change their systems or processes overnight.

In terms of upskilling your personnel, there are free resources available, such as e-training modules that don't take long to complete. Wherever possible the Ministry will share useful resources, such as cyber security week resources with providers.

Will the guidelines be reviewed? and will the Ministry's expectations change in the future?

Absolutely. We will need to monitor and review the guidance over time to ensure it is relevant and appropriate for providers.

It is possible that some of the IT controls we have identified may become higher, or lower, priority in the future as technologies, practices and costs change.

In February 2021 we will review any feedback we receive after the draft guidelines come into effect on 1 December 2020, and re-issue the guidelines if necessary.

privacy@justice.govt.nz