information and privacy commission new south wales

IPC Data Breach Guidance

May 2018

Contents

1. Data Breaches and Notification

1.1. What is a data breach?

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to your Agency's data. Although malware, hacking and data theft are usually the first examples of data breaches that come to mind, many breaches are a result of simple human or technical errors rather than malicious intent.

The accidental loss of a paper record, laptop, or USB stick may constitute a data breach under NSW regulation, as would emails sent to the wrong recipients if they contained classified material or personal information. Data breaches can also occur if authorised system users access restricted information for unauthorised reasons, such as employees looking up Agency-held information for personal reasons. Agencies should take a broad approach when thinking about the types of data breach that may occur in their organisation.

Some data breaches are serious and can potentially harm individuals and agencies whose information is breached. While NSW does not currently have a mandatory notifiable data breach reporting requirement, the Privacy Commissioner has a voluntary reporting scheme in place. The voluntary scheme encourages agencies that have experienced a serious data breach to report the details of the breach to the Privacy Commissioner, so that the Privacy Commissioner can assess the breach, provide advice or investigate.

1.2. What are the benefits of reporting a data breach?

If you identify that a data breach has occurred, there are significant benefits in being proactive in reporting:

- It demonstrates to your clients that you have processes in place to identify and manage data breaches, and that these are deployed without delay to minimise any potential damage
- The process of assessment, notification and remediation will strengthen data breach and privacy processes, preventing future breaches and minimising risk to your Agency
- It reinforces the importance that your Agency places on accountability for the protection of personal information internally to your staff, to promote a privacy positive culture
- It demonstrates to the public that your Agency views the protection of information as a priority, helping to maintain public trust.

1.3. What are the potential impacts of a data breach?

The impact of a data breach depends on the nature and extent of the breach and the type of information that has been compromised. Some breaches may involve only one or two people while others may affect hundreds or thousands. Larger breaches expose a wider group of people and could require considerable

notification and remediation activities. However it is not only the initial size of the breach that determines its impact. If there is a breach of sensitive or confidential information, reputational and financial harm can occur for the Agency itself, Agency staff, as well as the Government. There have been cases of breached information being used to derail programs of work and undermine professional relationships.

Serious impacts of a data breach could include:

- Risk to individuals' safety
- Financial loss to an individual or organisation
- Damage to personal reputation or position
- Loss of public trust in an Agency or the services it provides
- Commercial risk through disclosure of commercially sensitive information to third parties
- Threat to an Agency's systems, impacting the capacity to provide services
- Impact on Government reputation, finances, interests or operation.

Breaches of personal data can result in significant harm, including people having their identities stolen or the private home addresses of protected or vulnerable people being disclosed. In some circumstances, this can expose an individual to a significant risk of harm. As such, even a breach affecting a small number of people may have a large impact. Agencies should assess the specific risks based on the type of data they hold, and the specific circumstances surrounding the data breach.

Agencies should also consider the risks that could result from data breaches:

- that result in a loss of data integrity,
- where information is maliciously altered, or a loss of availability,
- where data may not be disclosed, but is rendered inaccessible, with potentially harmful consequences for individuals.

1.4. How do I determine how serious a breach is?

Determining the seriousness of the breach affects what response actions should be taken and whether the breach should be reported or not. There is no objective measure of seriousness, and agencies should work out what constitutes a serious breach by:

- considering the type of data held,
- whether personal or health information was disclosed,
- the number of individuals affected, and
- the risk of harm that could be caused to both individuals and the Agency by the breach.

In assessing seriousness of the breach, the Agency should consider:

- The type of data that has been breached – does it include financial, health or other sensitive categories of data? Are there other characteristics of the data that could pose a high risk (e.g. commercial information that could pose a reputational risk to an Agency or other organisation)?
- The data context – does the breach affect data that would normally be publically available, or is the data known to be very poor quality that if used could create risk to individuals?
- How easy would it be for individuals to be identified from this data?
- The circumstances of the breach – for example, was it a single incident (such as the loss of a USB or laptop) or a malicious attack that poses an ongoing risk, or was data altered in a way that it would pose a risk to the individuals to whom the data relates?

It is recommended that agencies implement a process to assess seriousness so that a risk threshold can be applied to data breach protocols.

The following case studies provide an illustration to demonstrate how the seriousness of a breach may be assessed:

Data Breach Case Studies

Case study 1: Mail merge problem

A mail-merge problem at a large government Agency has resulted in emails being sent to the wrong recipients. The subject of the email was a retirement party being held for an outgoing employee and the email included details about the employee, the date and location of the party, and the contact details of the sender. After a brief look at the recipients list, it was seen that the email was accidentally sent to unintended internal business teams, as well as a few external consultants.

In this case, while information was sent to a reasonable number of unintended recipients, the consequences are limited to some potential embarrassment caused to the retiring employee and a minor level of reputational damage that may result from the external consultants identifying that a mistake has been made. This would not constitute a serious breach and should be handled internally. Reporting to the Privacy Commissioner is not recommended in this case. Actions may include apologies being sent out and the mail merge problem being addressed.

Case study 2: Lost Laptop

The daughter of staff member at a smaller regional council had her laptop computer stolen at a university library. Upon hearing about this, the staff member remembered having used the daughter's laptop during a conference and suspected that the laptop still had copies of unsecured spreadsheets containing sensitive information on the computer's desktop. This information included account access, financial and personal information about council staff. The daughter was not sure whether the laptop was password protected. In the hope of recovering the laptop, the staff member waited until the police investigation was over before reporting the breach to management.

This would be considered a serious breach and should have been reported to the council immediately and then in turn to the Privacy Commissioner. A combination of factors, including the fact that the laptop is a personal device and unable to be monitored or secured by council IT staff, the sensitive nature of

the information that has been compromised and its potential for misuse, and the uncertainty around the security setting on the laptop itself, and the long length of time between when the breach occurred and when it was identified by the council, all contribute to the likelihood that serious harm could occur. The lack of immediate notification to the council means that steps to potentially isolate and mitigate damage could not have been taken. The Privacy Commissioner's assessment would look at the details of the breach, the actions taken in response to the breach, and would potentially suggest improvements to staff training, device-use policies and data breach response plans.

1.5. What do I do if I identify that a data breach has occurred?

The immediate actions taken once a data breach is suspected or identified are crucial in minimising the harm that the data breach could cause. Assemble a Breach Response Team to manage the process, which should include Executive decision makers, information management and technology/security, the Privacy Manager/Officer and Communication staff.

The following steps should be followed to manage a data breach when it occurs:

- *Contain* – All necessary steps possible should be taken to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that led to the breach, or revoke or change access codes or passwords.
- *Evaluate* – Assess the type of data involved in the breach, and the risks associated with the breach, to determine next steps. Consider the type of data breach, who is affected, what caused the breach, and what are the specific risks that could follow. This should be a broad scope assessment of the breach and may include looking at external systems, website and storage drives if they were a factor in the breach. For example, a breach of a combination of data types will typically create a greater potential for harm than a single data type.
    - **Who is affected by the breach?** The assessment may include reviewing whether individuals and organisations have been affected by the breach, the level of sensitivity of the data that is affected, how many individuals and organisations have been affected, and whether any of the individuals have personal circumstances which may put them at particular risk of harm.
        - **What was the cause of the breach?** The assessment may include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Was it a one-off incident or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data been recovered? Is the data encrypted or otherwise not readily accessible?
        - **What is the foreseeable harm to the affected individuals/organisations?** The assessment may include reviewing what possible use there is for the data. For example, could it be used for identity theft, threats to physical safety, financial loss, or damage to reputation? Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online?

- *Notify* – While not compulsory in NSW, notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations and reflect positively on an Agency's reputation. By notifying, you are enabling individuals to take any steps required to protect themselves from risk that may occur as a result of the data breach. In general, if a data breach creates a risk of harm to an individual/organisation, the affected individual/organisation should be promptly notified.

  Individuals and organisations affected by the breach should be notified as soon as practicable. Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach. Notification should be done based on the assessment undertaken in the step above.

  Notification may also include reporting the breach to the Privacy Commissioner. This is a voluntary step but is encouraged for serious breaches. Reporting of a serious breach allows the Privacy Commissioner to assess the circumstances and impact of the breach and provide feedback on the appropriateness of the remedial actions.

  Agencies should have documented procedures to assist staff to know when to notify, what process to follow, and who is responsible for each action involved.

- *Act* – Implement any additional actions that you have identified to mitigate risks. This could include actions such as initiating take down orders on external websites or putting processes in place to assist individuals who have been affected by the breach.

- *Prevent*– Put into action preventative efforts, based on the type and seriousness of the breach. This may include a security audit of both physical and technical security controls, a review of policies and procedures, a review of employee training practices or a review of contractual obligations with contracted service providers. If the breach has been reported to the Privacy Commissioner, further preventative and remedial actions may be recommended subsequent to the Privacy Commissioner's assessment.

These five steps should be integrated into the policies, procedures or Privacy Management Plans of an Agency to help ensure responses to data breaches are consistent and easily and quickly put into action.

For a more detailed description of these steps, and an example of how they may be integrated as part of a data breach policy see the IPC's Data Breach Policy. It includes templates for notification letters and action plan. Agencies should refine the guidance to suit the specific operation and structure of their agencies.

1.6. What is the role of the IPC? What happens when I report a breach?

The IPC's role is to uphold and protect information and privacy rights in NSW. If a data breach has been reported by an Agency, the NSW Privacy Commissioner, or delegate, conducts an assessment of the notification to check the circumstances of the breach. The assessment examines all relevant causes and considers what steps have been taken by the Agency in response and the short or long-term measures that could be taken to prevent any recurrence. The Privacy Commissioner, or delegate, may seek further information from the Agency to inform the assessment; this may include further details, or requesting a

meeting to clarify information. Following the assessment, the Privacy Commissioner will write to the Agency outlining any actions the Privacy Commissioner proposes to take or that the Agency is asked to take. This may include undertaking an audit or an investigation.

When notifying, the Privacy Commissioner requests similar information to that which would be provided to individuals or organisations affected by the breach. The personal information about the affected individuals is not required.

It may be appropriate to include:

- a description of the breach
- the type of personal information involved in the breach
- what response has been made to the breach
- whether any longer term mitigation is to proposed/intended
- what assistance has been offered to affected individuals
- the name and contact details of the appropriate contact person, and
- whether the breach has been notified to other external contact(s).

The Privacy Commissioner will report in a de-identified form the number of voluntary data breach notifications that have been reported.

More information can be found on the IPC website

1.7. Data breach procedures and notification – Frequently Asked Questions

1.7.1. If a significant data breach occurs in a State Owned Corporation, who should I notify?

State Owned Corporations, while not directly covered by either the PPIP Act or the Commonwealth Privacy Act, are encouraged to follow the same processes as State Government Agencies and notify the IPC in the event of a breach.

1.7.2. If more than one Agency holds the same records, should all Agencies notify?

If two or more Agencies hold the same records and a data breach occurs (for example, if a data breach occurs impacting records of children in Child Protection services who are receiving joint services from FACS, Health and Education), one Agency should take responsibility for notifying the breach to the affected individuals and the Privacy Commissioner. Ideally, the lead Agency which has the closest relationship to the affected individuals should take responsibility for notifying.

1.7.3. Our Agency outsources services for our clients to Non-Government Organisations (NGOs) – if there is a data breach, who should manage the response?

The lead Agency should manage the assessment of the cause of the data breach and monitor the implementation of any remediation actions put in place to prevent a recurrence of the issue.

If it is a serious breach and notifications to the individuals affected are required, ideally the notifications should be made by the NGO that has the closest relationship with the individual. The NGO should also consider any reporting requirements it may have under any other legislation that has application to them. For example the Commonwealth Notifiable Data Breaches Scheme.

1.7.4. Our systems are managed by a third party contacted service provider - if there is a data breach, who should manage the response?

In this situation, the contracted service provider should conduct the assessment and, if the cause of the breach originated within their facilities/technical environment, determine the appropriate remediation actions that should be implemented. If the breach was the result of human behaviour within the Agency (for example, staff in a hospital inappropriately accessing the records of patients that they have no professional association with), the Agency should take action. It is more appropriate for notifications to affected individuals to be made by the Agency that has the direct relationship with the individual.

1.7.5. Should I notify the NSW Police about the data breach?

NSW Police should be informed if your assessment of the data breach identifies that the cause is cybercrime or other theft (e.g. theft of laptops that had personal information stored on them). Details of the breach should not be made public if NSW Police, or any other law enforcement body, are investigating the breach, without consultation with the Police.

1.7.6. Are there any circumstances where I should notify any other external Agency?

Depending on the circumstances of the data breach and the categories of data involved, there may be requirement to notify other Agencies, such as:

- Financial services providers
- Police
- The Australian Taxation Office
- The Australian Digital Health Authority
- The Department of Health
- Department of Finance, Service and Innovation
- The Office of the Government Chief Information Security Officer
- The Australian Cyber Security Centre
- Professional associations, regulatory bodies or insurers

1.7.7. What is the impact of the GDPR data breach notification requirements on my Agency?

The European Union's General Data Protection Regulation will apply from May 2018. This regulation will affect any Agency offering goods or services to, or monitoring the behaviour of individuals in the European Union (EU), such as agencies selling tickets to attractions or events online to individuals in the EU, and educational facilities offering programs to students located in the EU.

The GDPR has mandatory notification requirements in the event of a data breach. Normally notification is made to the data protection supervisory authority of the particular EU country the breach occurs in. The difficulty for Australian organisations that hold information about EU residents but who do not have an established presence on the ground in any particular EU country is the absence of an agreement of to whom the notification should be sent. This is an issue that has been noted by the EU Working Group but which remains unresolved.

Organisations that believe they may have notification obligations under the GDPR should review the advice provided by the Office of the Australian Information Commissioner (OAIC) for government agencies and Australian businesses.

1.7.8. Data sovereignty – if our Agency releases data to a law enforcement body, is that a data breach?

Data sovereignty is a complex issue and it is unclear where the boundaries lie with regard to when organisations are obligated to provide data to law enforcement agencies. Whenever data is requested in this way, it should be clear what the legal basis for the provision of that data is. If this is not clear, agencies should request clarification before providing the data. In most cases, organisations are compelled to provide data to law enforcement agencies and this would not be considered a data breach. Agencies should seek advice from their Agency Privacy Officer if they are unsure about a request that has been made for law enforcement purposes.

In cases where the request comes from law enforcement agencies outside Australia, organisations should seek legal advice before providing that data. Where data has been provided without a clear legal basis it is recommended organisations treat this as a breach and follow data breach procedures accordingly.

1.8. Other Legislative/Regulatory Obligations

It is important that agencies are aware of any legislative or regulatory requirements around data protection and the reporting of data breaches. Particular requirements will differ from Agency to Agency depending on the type of data that is held, and Agency specific legislation. Agencies should develop an understanding of which requirements are applicable to them. Below is a selection of requirements that NSW agencies should be aware of:

NSW Government

- For instances when personal information is breached, requirements under the *Privacy and Personal Information Protection Act 1998* include conducting a privacy internal review if a request is received from an individual, as well as co-operating with any enquiries by the Privacy Commissioner. More information can be found on the IPC website.
- For instances when health information is breached, the *Health Records and Information Privacy Act 2002* states that agencies may be required to perform a privacy internal review of the breach and co-operate with the Privacy Commissioner. More information can be found on the IPC's website.
- For instances where information shared from other NSW Government agencies which include health information or personal information is breached, the *Data Sharing* (Government Sector) *Act 2015* requires that both the data provider and the Privacy Commissioner be notified as soon as practicable. More information can be found on the NSW ICT Strategy website.

Australian Government

- For breaches involving tax file numbers (TFN), which may result in serious harm, NSW Government agencies are required under the federal Notifiable Data Breaches scheme to report the breach to the Office of the Australian Information Commissioner (OAIC). More details about reporting TFN breaches can be found on the IPC's NSW Public Sector Agencies and Notifiable Data Breaches factsheet.
- For breaches or potential breaches of My Health Record information, there is a requirement in the federal *My Health Records Act 2012* to notify either the OAIC, the My Health Record System Operator, or both, depending on the capacity in which your Agency holds the data. The full details about My Health Record can be found at the My Health Record website.

International

- For breaches involving personal data about individuals in the European Union, agencies may be subject to a requirement in the EU's General Data Protection Regulation (GDPR) that the relevant supervising authority (the OAIC) be notified, where feasible, within 72 hours of the breach. For full details about reporting and GDPR requirements see the OAIC's website which provides information for agencies and Australian businesses.

1.9. Where can I go to for more information?

For more information on data breaches, and on information management and privacy advice in general, you can access the resources published by the IPC on the IPC website. These include detailed guidelines, factsheets, checklists, example policies and generic forms aimed at supporting privacy and information access rights and management processes in public sector agencies.

The following resources provide additional information relevant to agencies:

- IPC Data Breach Policy
- IPC Mandatory Data Breach Notification Scheme Factsheet

- IPC Guide to Privacy Management Plans
- IPC Governance Framework

In addition to the IPC resources, the federal OAIC website provides resources for agencies and individuals on good privacy and information protection practices.

For information about the implementation of practical IT cybersecurity controls, see the advice from the Australian Cyber Security Centre, including the Essential Eight baseline for mitigating cyber security incidents.

For information specific to your Agency, contact your Agency's Privacy Contact Officer or consult your Agency's Privacy Management Plan which should be made available on the public website, or by request.

2. Best practice in preventing and responding to breaches

2.1 Executives

For good privacy practices to be effectively integrated into an Agency, they should be supported and championed by those at the top of the Agency.

2.1.1 Good prevention practice

People/Culture

- Support and advocate a privacy positive culture. Don't delegate to a specific business unit, such as IT or legal. Make the business aware that the executive and board consider privacy a priority.
- Understand the privacy risks of your Agency and maintain strong and open vertical communication channels about privacy and data protection issues.
- Change the view that data breaches are inherently catastrophic, as this discourages the reporting of breaches internally and results in reactionary and ad-hoc instead of proactive practices.
- Understand the scope and impact, including reputational, financial and physical harm, of data breaches. Recognise the variety and varying severity of potential data breaches.
- Establish a data breach policy and communicate the policy and the key contacts for advice within the Agency.
- Establish a data breach response team. The OAIC provides guidance on the skills required and recommended membership for the response team.

Processes

- Establish a data breach response plan for your Agency that defines strategies to contain and mitigate data breaches, and clearly defines responsibilities, reporting processes and the communication strategy to be put into place to advise individual and relevant entities of the breach.
- Establish metrics-based privacy and data protection reporting processes. This ensures that the executive and board-level positions are aware of the Agency's privacy maturity as well as reinforces to the wider Agency that there is a commitment to improving privacy practices and addressing data breaches.
- Support managers and staff by maintaining clear, considered and strong governance structures which make monitoring and response actions transparent and understood by all staff.
- Encourage the incorporation of data breach processes into all common processes.
- Develop a data breach response plan that includes all levels of the Agency.

Policy

- Identify how privacy, data protection, and data breaches are best integrated in your Agency's policy suite. Ensure that such policy is effective and meaningful to the way your Agency works.
- Ensure that data governance arrangements address sensitive data and other areas of high-risk.

Technology

- Encourage an Agency-wide understanding of how data is stored in the IT network and where the vulnerabilities lie.
- Encourage architectural-level reviews of applications and systems for data breach prevention purposes.
- Ensure that ongoing audit and monitoring processes are in place.

2.1.2 Good response practice

Immediate actions

- Confirm that data breach procedures are being followed and monitor the situation as it unfolds.
- Be responsive to communications about the breach to ensure you have available the appropriate level of detail to assess the nature and impact of the breach.

Notification

- Based on the nature of the particular breach, decide whether you will report it to the Privacy Commissioner. Reporting should be done in cases of serious breaches and it is encouraged that the Agency CEO is responsible for the report itself.
- If reporting, develop and send, as soon as practicable, a report to the Privacy Commission which includes details about the breach and actions taken to contain it. An example of what should be included in the report can be found in the IPC's own Data Breach Policy.

- Support internal communication actions and, if applicable, the notification of individuals whose personal data has been breached.

Review

- Ensure that review procedures are being followed and, if necessary, that an assessment of the breach and the response actions taken be disseminated to all relevant individuals.
- If an investigation is underway, support the investigation by supply ongoing information as it progresses.
- Follow-up on any recommended actions and incorporate lessons learnt into the understanding on your Agency's data breach risk profile.
- If necessary, conduct audits to ensure follow-up actions and improvements are being implemented.

2.1.3 Resources

- IPC Data Breach Policy
- IPC Guide to Privacy Management Plans/Governance Framework
- OAIC Data breach preparation and response

2.2 Managers

Managers have a role in supporting staff to follow data breach prevention practices, as well as acting quickly in the event of a data breach. The actions and responsibilities of managers straddle the policy and operation sides of data breach prevention and response.

2.2.1 Good prevention practice

People/Culture

- Understand your data environment. Know what data you collect, how and where it is stored and who should have access to it. Understand the risks that are particular to your Agency's circumstances.
- Encourage a privacy aware culture among teams. Make privacy and data breach considerations part of shared everyday practice, instead of addressing concerns ad hoc.
- Provide meaningful privacy and data training for staff, relevant to their role.
- Support staff in taking privacy policy actions and encourage internal notification and reporting of privacy and data protection concerns.
- Make sure that privacy and data protection responsibilities are well known and that privacy governance structures are adhered to, including identifying who is responsible for escalation.
- Be aware of staff working arrangements, as they may impact on how staff access and transfer data. Ensure that current arrangements do not encourage staff to circumvent privacy policy and data protection practices.

Processes

- Based on your understanding of risks to your data, incorporate privacy-positive and data protection practices into standard processes.
- Encourage a culture that promotes awareness of privacy responsibilities and supports the reporting of privacy breaches by making reporting processes clear and visible to all staff.
- Review processes routinely in order to accommodate changes to the privacy risk profile of the Agency, and to incorporate lessons learnt from privacy incidents that have occurred across government.
- Ensure that standard processes are followed and that staff are aware of data protection-specific processes.
- Develop standard assessment criteria to evaluate the severity and impact of potential data breaches.
- Develop robust and clear operation plans and procedures in order to make responding to suspected breaches routine and thorough.

Policy

- Make sure that privacy and data protection is incorporated into policies in a way that is appropriate to the way your Agency works and the data it holds.
- Understand how policy relates to the particular data breach scenarios your Agency is likely to face.
- Communicate policy with staff and receive feedback in order to ensure that policy remains relevant and effective.

Technology

- Ensure that Bring your Own Device (BYOD) and portable data storage use complies with Agency privacy policy.
- Discourage practices that involve circumventing technological controls on data storage, use, copying and transfer. Make sure that technology arrangements support staff practices so staff do not have to find workarounds.
- Ensure that protections are in place 24 hours a day, which may require automation of security alerts.
- Ensure that access controls are in place and that access is deactivated for exiting staff.
- In addition to identifying external threats such as malware, keep access audit logs and ensure that they are monitored for inappropriate and unauthorised data access.

2.2.2 Good response practice

Immediate actions

- Establish quickly the key details of the breach, including when it occurred or was identified, how it occurred, what data was affected and the extent of the breach.

- Act as soon as possible to contain the breach. This may involve shutting down of applications, closing of accounts, changing of passwords, locating missing items, or restricting access rights.
- Perform a preliminary assessment of the potential harm that may result from the data breach in order to identify who should be contacted and how urgent the situation is.
- Inform all relevant parties in line with your Agency's data breach procedures and involve relevant parties in the containment and evaluation actions.

Notification

- If it is established that the breach is serious in nature, escalate the issue as soon as possible, according to the data breach procedures of your Agency.
- If the notification of data subjects is necessary, ensure that this process has the support of the Agency and follows Agency guidelines. Use the information you have gathered in the evaluation stage to prepare the response.

Review

- Document the detail of the data breach and the subsequent actions taken and, depending on the seriousness of the breach, conduct a full investigation of the causes and consequences of the breach.
- Provide guidance and oversight for ongoing harm mitigation exercises.
- Assess the appropriateness of the response to the breach and identify lessons learnt and where improvements could be implemented.
- Incorporate improvements and lessons learnt into policy, procedures, training and practices. Communicate any changes with staff.
- Provide regular reports to the executive and board about data breach incidents.

2.2.3 Resources

- IPC Data Breach Policy
- IPC Mandatory Data Breach Notification Scheme
- IPC Privacy Management Plan Guide and Checklist
- OAIC Data breach preparation and response

2.3 Staff

Staff are at the front line when it comes to preventing and responding to data breaches. Staff should make sure they are following effective data breach prevention behaviours and maintaining open communication with managers to ensure practices and policy are easy to follow and effective in action. Staff are often the first to become aware of a data breach, and therefore will be vital in responding quickly.

2.3.1 Good prevention practice

People/Culture

- Make sure you're aware of your Agency's privacy principles as well as the types of breaches that might affect your Agency.
- Identify the individuals in your Agency responsible for privacy and data protection. These are the staff members who will provide support for understanding and implementing data breach prevention practices, as well being the contact points in the event that you identify as suspected breach.
- Establish honest and consistent privacy and data breach communication channels with managers and other staff.

Processes

- Ensure that you are aware of proper processes and that they are followed.
- If you identify where privacy and data protection improvements to processes can be made, communicate this with management.
- Minimise the transporting and copying of data in common processes, especially if this is done using portable devices, email, or syncing files to local devices.

Policy

- Be aware of privacy and data protection policies and abide by them. Provide feedback on policy that is difficult to implement so that it may be improved.
- Relevant policies include those that cover computer and email use, BYOD, information access restrictions and conditions, and personal information collection and use.

Technology

- Abide by the data protection policies and practices of your Agency with regard to the use of computer, emails and other electronic devices.
- Ensure that security protections, such as passwords and two-factor authentication are compliant with your Agency's rules.
- Avoid transferring data through insecure methods, such as USB-sticks, paper copies, unencrypted attachments to emails.
- Keep applications on your devices updated to the latest version, as vulnerabilities are frequently patched.
- Be aware of the data you hold on your computer and your devices. Avoid replicating data across multiple devices, especially is they are portable and may be lost, stolen or misplaced.

2.3.2 Good response practice

Immediate actions

- Establish quickly the key details of the breach, including when it occurred or was identified, how it occurred, what data was affected and the extent of the breach.
- Advise the relevant manager, or breach management team, of the breach as soon as possible, according to your Agency's procedures. Do not wait until you have collected all the key details before you start communicating with them.
- Act as soon as possible to contain the breach. This may involve shutting down of applications, closing of accounts, changing of passwords, attempting to locate missing items, or restricting access rights.

Notification

- Maintain ongoing communication with managers and other relevant staff about the consequences and follow-up activities that result from the breach.
- Follow directions on notification from management. This may involve you making contact with data subjects directly, especially if the breach involves only a small number of individuals. You should receive guidance on what details the notification should include.

Review

- Help implement any lesson learnt and improvement in your everyday practice.
- Assist with any investigation and review exercises. Provide meaningful and honest insight into the breach.

2.3.3 Resources

- IPC Data Breach Policy
- OAIC Guide to securing personal information
- OAIC Data breach preparation and response

3. References

Data Breaches and Notification

- IPC's Data Breach Policy: http://ipc.nsw.gov.au/sites/default/files/file_manager/IPC_Data_Breach_Policy_Nov_2016_ACC.pdf

- Resources for public sector agencies on IPC website: https://www.ipc.nsw.gov.au/resources-public-sector-agencies
- Advice provided by the Office of the Australian Information Commissioner (OAIC) for government agencies: https://www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/government-agencies/does-the-eu-general-data-protection-regulation-gdpr-apply-to-australian-government-agencies
- Advice provided by the Office of the Australian Information Commissioner (OAIC) for Australian businesses: https://www.oaic.gov.au/media-and-speeches/news/general-data-protection-regulation-guidance-for-australian-businesses
- More information about conducting a privacy internal review under the *Privacy and Personal Information Protection Act 1998* : https://www.ipc.nsw.gov.au/ppip-act
- More information about conducting a privacy internal review under the *Health Records and Information Privacy Act 2002:* https://www.ipc.nsw.gov.au/hrip-act
- More information about data sharing on NSW ICT Strategy website: https://www.finance.nsw.gov.au/ict/nsw-data-analytics-centre/data-sharing-legislation
- More details about reporting TFN breaches in IPC's NSW Public Sector Agencies and Notifiable Data Breaches factsheet: https://www.ipc.nsw.gov.au/fact-sheet-nsw-public-sector-agencies-and-notifiable-data-breaches-1
- More details about My Health Record: https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/notifications-of-data-breaches
- More information for agencies about reporting and GDPR requirements on the OAIC's website: https://www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/government-agencies/does-the-eu-general-data-protection-regulation-gdpr-apply-to-australian-government-agencies
- For full details about reporting and GDPR requirements see the OAIC's website which provides information for Australian businesses: https://www.oaic.gov.au/media-and-speeches/news/general-data-protection-regulation-guidance-for-australian-businesses
- For more information on data breaches, and on information management and privacy advice in general, you can access the resources published by the IPC on the IPC website: https://www.ipc.nsw.gov.au/resources-public-sector-agencies
- IPC Data Breach Policy: https://www.ipc.nsw.gov.au/sites/default/files/file_manager/IPC_Data_Breach_Policy_Nov_2016_ACC.pdf
- IPC Mandatory Data Breach Notification Scheme Factsheet: https://www.ipc.nsw.gov.au/sites/default/files/file_manager/IPC%20Fact%20sheet%20-%20Mandatory%20Data%20Breach%20Notification%20Scheme.pdf

- IPC Guide to Privacy Management Plans: https://www.ipc.nsw.gov.au/privacy-management-plans
- IPC Governance Framework: https://www.ipc.nsw.gov.au/privacy-governance-framework
- In addition to the IPC resources, the federal OAIC website provides resources for agencies and individuals on good privacy and information protection practices: https://www.oaic.gov.au
- For information about the implementation of practical IT cybersecurity controls, see the advice from the Australian Cyber Security Centre: https://www.acsc.gov.au/publications.html
- Essential Eight baseline for mitigating cyber security incidents: https://www.asd.gov.au/publications/protect/Essential_Eight_Maturity_Model.pdf

Best practice in preventing and responding to breaches

- The OAIC provides guidance on the skills required and recommended membership for the response team: https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response#part-1-data-breaches-and-the-australian-privacy-act
- An example of what should be included in the report can be found in the IPC's own Data Breach Policy: https://www.ipc.nsw.gov.au/sites/default/files/file_manager/IPC_Data_Breach_Policy_Nov_2016_ACC.pdf
- IPC Data Breach Policy: https://www.ipc.nsw.gov.au/sites/default/files/file_manager/IPC_Data_Breach_Policy_Nov_2016_ACC.pdf
- IPC Guide to Privacy Management Plans/Governance Framework:https://www.ipc.nsw.gov.au/sites/default/files/file_manager/PGF_August_2016_FINAL_1.pdf
- OAIC Data breach preparation and response: https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response
- IPC Mandatory Data Breach Notification Scheme: *https://www.ipc.nsw.gov.au/fact-sheet-nsw-public-sector-agencies-and-notifiable-data-breaches-1*
- IPC Privacy Management Plan Guide and Checklist: *https://www.ipc.nsw.gov.au/privacy-management-plans*
- OAIC Data breach preparation and response: https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response
- OAIC Guide to securing personal information: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information
- OAIC Data breach preparation and response: https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response