How to design and implement a data retention and destruction program in six steps

Allens Linklaters | 200

A WAKE-UP CALL

While all the facts surrounding the Optus and Medibank cyber incidents have yet to emerge fully, one thing is clear: *the best way to avoid or reduce the impact of a data breach is not to have the data in the first place*.

So ask yourself: has your organisation collected more data than required, and kept it for *longer* than necessary? What steps should your organisation take to accelerate, or even initiate, a data retention and destruction program?

As in-house counsel or compliance specialists, you will likely find yourself tasked with the job of helping to implement such a program. If you're not, you should be.

There are over 100 federal and state laws that impose data retention requirements of varying lengths, so legal input is critical. It is *already mandatory* for organisations subject to the Privacy Act to destroy or de-identify personal information once it is no longer required. The Office of the Australian Information Commissioner has been focused on breaches of this obligation for some time.

This practical guide has been designed to help you navigate the regulatory, operational and technical complexities you are likely to face, and identifies six steps you can take now.

Key takeaways

1

Just because you can, doesn't mean you should.

Data presents exciting opportunities to personalise offerings, automate processes and extract other benefits. This needs to be balanced, however, with the risk of collecting and keeping such data.

2

Organisations need to comply with regulatory requirements to retain and destroy data.

Given the volume of these requirements, it can be hard to determine which laws apply to what records and which should take precedence where there are inconsistencies.

3

Keeping records and data for longer than required is not just a regulatory risk, it presents a significant operational, reputational and cyber risk.

Securely destroying data can help mitigate these risks and costs if you do have a data breach.

4

Regulators (eg OAIC, ASIC and APRA) expect organisations to have good governance around records management.

This includes:

a. having policies and procedures in place to monitor and ensure compliance with record management obligations;

b. ensuring staff are aware of these measures; and

c. testing those measures.

5

Change is coming.

Following the Optus data breach, we expect more prescriptive requirements around the destruction or de-identification of personal information (particularly information collected for ID verification) will be introduced, including higher penalties for a breach.

There have also been calls to introduce a right for individuals to request that their personal information be destroyed.

The current challenge

1. So much data

Organisations have more data than they know what to do with. The more data an organisation handles, the greater the risk exposure and the more difficult (and expensive) it becomes to tag, monitor, secure and (when it is no longer required) destroy, on an ongoing basis.

2. Complex regulatory landscape

The regulatory pressure continues to build, and organisations must navigate and apply overlapping and often inconsistent laws to business records.

For example, many of the 100 federal and state laws covering this area impose different retention periods—from the Corporations Act, to tax and employment laws, to laws designed to combat money laundering and sector-specific obligations.

3. Increased regulator scrutiny

The Privacy Act requires that organisations destroy or de-identify personal information when it is no longer required. Other laws (like the Tax Administration Act, Superannuation Industry (Supervision) Act and state health records laws) also require organisations to destroy specific types of information (like TFNs or health information).

Industry organisations may also mandate deletion of certain information—like the Payment Card Industry Data Security Standard which requires destruction of credit card details.

Even before the current Optus data breach, the Office of the Australian Information Commission has increasingly focused on compliance with APP 11.2, including two recent determinations against organisations found to have breached the principle.

A failure to destroy or de-identify personal information once it is no longer required can also lead to a finding that an organisation has not complied with its obligations to:

- have policies and procedures in place to enable it to comply with the APPs (APP 1.2); and
- take reasonable steps to protect personal information (APP 11.1).

4. Technical constraints

System limitations and data structures can make it difficult to implement data retention and deletion requirements. For example, legacy systems may not permit the destruction of data with sufficient granularity, and it can be hard to identify data within unstructured datasets (eg email).

> *Australian Privacy Principle 11.2 requires that organisations take reasonable steps to destroy or de-identify personal information where that information is no longer required for any permitted purpose and does not otherwise need to be retained under Australian law.*

Balancing the risks

A comprehensive and considered data retention and destruction program will require you to balance the concurrent risks of failing to retain data when required and also holding it longer than necessary.

Risks of not retaining data when required

- Breach of regulatory record retention requirements (including associated penalties)
- Inability to access information needed to respond to claims
- Committing an offence, or being found in contempt of court, if records relating to current or anticipated legal proceedings are destroyed
- Restricts legitimate business uses and operations

Risks of retaining data longer than necessary

- Breach of the Privacy Act and other obligations which require destruction of certain records (including associated penalties)
- Increased risk of data breaches and associated consequences
- Increased data storage costs
- Becomes harder over time to delete or destroy data and to identify what should or should not be retained

Your six-step guide

STEP 1: KNOW YOUR DATA

ASK

What data do we hold and why?

PARTICIPANTS

Project lead, Legal, Compliance and key stakeholders in each business unit.

TOOL

Data questionnaire (to be completed by key stakeholders) to help identify the categories of records held in each business unit and the purposes for which those records are held.

ACTION

- Identify the categories of records that are held by your organisation.
- For each category of record:
  - consider the purposes for which those records are held—eg business purpose, to comply with contractual obligations or to assist in defence of third party claims; and
  - test whether those records need to be retained for those purposes and, if so, in what form.

PRACTICAL TIPS

- Data/records may be in hard copy (including storage sites) or electronic (on systems or backup tapes) and may be in structured or unstructured form. The longer your organisation has been operating, the more places data or records could be—from forgotten share drives to legacy or decommissioned (but not deleted) systems.
- If the records do need to be retained, consider whether they need to be retained in their entirety and also whether they could be stored on an aggregated basis or in de-identified form.

Your six-step guide

STEP 2: KNOW YOUR RETENTION OBLIGATIONS

ASK

Which records must be retained under law, industry standards or contracts (and for how long and in what form)?

PARTICIPANTS

Legal and Compliance.

TOOL

Regulatory mapping schedule which identifies, for each category of records, the applicable record retention requirements.

ACTION

- Identify retention obligations that apply to the types of records or data you hold, as well as any applicable *sector-specific* retention obligations.
- Consider whether there are any restrictions on the *form* in which you must retain records or data (eg are electronic copies of hard copy records sufficient?).

PRACTICAL TIP

- Don't forget to consider retention obligations that may be mandated by your contractual arrangements, customers or industry standards.

Your six-step guide

STEP 3: KNOW YOUR OBLIGATIONS TO DESTROY OR DE-IDENTIFY DATA

ASK

Which records or data must be destroyed or de-identified under law? When?

PARTICIPANTS

Legal and Compliance.

TOOL

Regulatory mapping schedule which identifies, for each category of records, the applicable destruction or de-identification requirements.

ACTION

- Identify any obligations to destroy or de-identify data or records.

PRACTICAL TIP

- In addition to the destruction and de-identification requirement under the Privacy Act, there may be other obligations to destroy or de-identify data or records under federal or state laws which may apply to you or the records you hold (eg the Tax Administration Act prohibits an organisation *maintaining* a TFN after it is no longer required).

Your six-step guide

STEP 4: DEVELOP OR UPDATE YOUR DATA RETENTION AND DESTRUCTION POLICY

ASK

How do we ensure we comply with our regulatory and other obligations to retain and destroy data?

PARTICIPANTS

Legal and Compliance.

TOOL

Data Retention, Destruction and De-Identification Policy.

ACTION

Develop or revise your Data Retention, Destruction and De-Identification Policy. This policy should outline how and when staff should be retaining, destroying and/or de-identifying the data you hold or *control* (whether hard copy or digital).

WHAT BELONGS IN A DATA RETENTION, DESTRUCTION AND DE-IDENTIFICATION POLICY?

CATEGORISING DATA

Your policy should identify:

- ☐ The types of data your organisation collects
- ☐ The purposes for which you collect, create, hold and disclose that data
- ☐ The retention periods applicable to each dataset or record

DEALING WITH DATA

Your policy should describe:

- ☐ Acceptable and unacceptable reasons for retaining data for longer than any regulatory retention period (eg the records relate to current or anticipated legal proceedings)
- ☐ How (on an ongoing basis) to identify and retain records related to current or anticipated legal proceedings
- ☐ How to destroy, delete or de-identify data (including expectations and requirements of third parties who are destroying, deleting or de-identifying your data)
- ☐ How to manage re-identification risk of de-identified data (and when de-identified data should be destroyed or deleted)
- ☐ Where applicable, how data should be identified and tagged to help automate the process of classifying, monitoring and destroying or de-identifying data

GOVERNANCE

Your policy should set out:

- ☐ Who is responsible for compliance with each part of the policy (eg a RASCI matrix)
- ☐ The process to be followed if an *exception* to the policy is required (eg because there are technical constraints on deleting data) — including the process for the periodic review of any exceptions
- ☐ How compliance with the policy (by the organisation and suppliers) will be monitored and audited

PRACTICAL TIP

- ■ Make sure any exceptions to the policy are recorded in a register, including the reason for the exception.

Your six-step guide

STEP 5: IMPLEMENT YOUR DATA RETENTION AND DESTRUCTION POLICY

ASK

- Where (including in what systems) is our data held?
- How do we identify and track datasets/records to ensure we are applying the relevant retention period?
- How do we securely delete or destroy data?
- Are there any technical constraints to implementation?
- What controls do we need to put in place to address those technical constraints?

PARTICIPANTS

Project lead, Compliance, Information Technology, Facilities or Records team responsible for hard copy records, Legal and key stakeholders from each business unit.

TOOL

Register of records / datasets, Data Retention, Destruction and De-Identification Policy (see Step 4).

ACTION

- Map all data within your organisation and data held by your third parties, classify those records and tag with relevant retention periods.

  Test this with all your business units.

  Identify where you have the *same* data across different data sources or forms.
- Create a register of records/datasets held, including the systems in which they are held, relevant retention period (both regulatory and business) and any applicable legal hold.
- Identify any technical constraints which might inhibit compliance with the policy or require an exceptions path.
- Ensure your third party arrangements give you control and oversight over the return, destruction or de-identification of data both within the term of the arrangement and on its conclusion.
- Educate staff on what your policy requires.

PRACTICAL TIPS

- Implementing your Data Retention Schedule and Policy can take time. You may want to prioritise destruction or de-identification of certain types of records (eg sensitive information or government identifiers), or target particular systems first.
- Tools exist which can scan your systems for certain types of data or personal information. These can provide a secondary method for mapping data.
- Don't forget about backups when considering where data is located and when it should be destroyed.
- This is a good time to check whether you are collecting more information than necessary, and if any processes can be implemented to limit the collection of unnecessary data.
- Make sure you diligence third party arrangements—don't just rely on contractual protections.

Your six-step guide

STEP 6: MONITOR, REVIEW AND ENFORCE YOUR POLICY

ASK

Are we complying with our policy? Is it scalable?

PARTICIPANTS

Compliance, Audit and Risk.

TOOL

Data Retention, Destruction and De-Identification Policy.

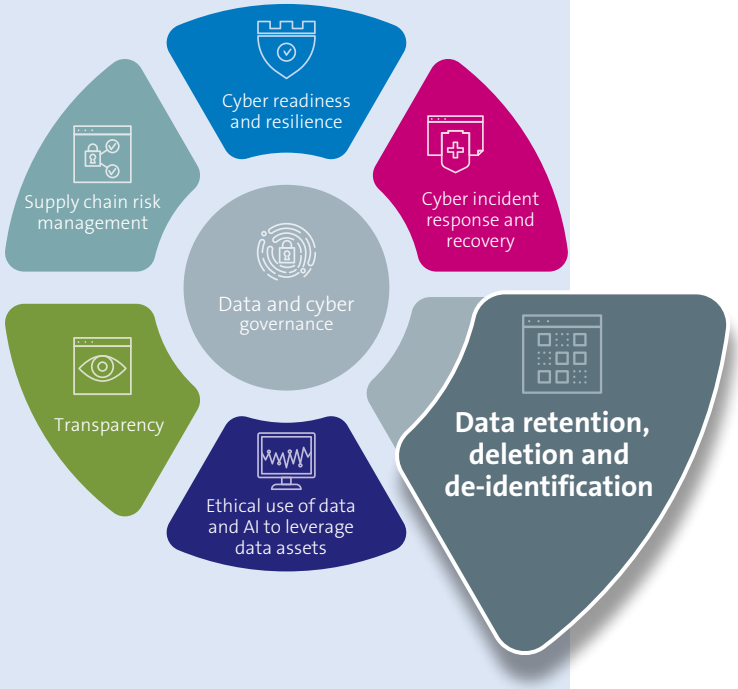
ACTION

- Actively monitor and audit compliance through both automated and manual processes.
- Ensure there is an active process to periodically review changes in records, systems and regulatory obligations.
- Ensure remedial actions identified as part of monitoring and audits are addressed.
- Where data has been de-identified, ensure the re-identification risk is monitored on an ongoing basis.

PRACTICAL TIPS

- Validate that records are in fact being deleted where required by the policy—whether by you or your third parties.
- A data breach of de-identified data may constitute a breach of personal information where it is capable of being re-identified (eg by combining it with other information available to the unauthorised recipient).

Questions your board should be asking



- ☐ Do we have a clear understanding of the data our organisation collects, generates and holds, *why* it collects that data and *where* it is held?
- ☐ Do we know all of our regulatory obligations to *retain* or *destroy* or *de-identify* that data?
- ☐ Have we identified *retention periods* for data, and do we have *processes* in place to ensure data is *securely destroyed* or *de-identified* following the expiry of those periods?
- ☐ How do we ensure that we are aware of proposed regulatory reforms and enforcement action that would impact our data retention and destruction program?
- ☐ How do we ensure we are complying with our Data Retention, Destruction and De-Identification Policy and related processes?
- ☐ What are the key risks and gaps in our data retention and destruction program?
- ☐ What processes do we have in place to ensure our data retention policy is regularly updated for changes to the data we hold, the reasons we hold them and the regulatory obligations that attach to them?

> *Boards need to have a thorough understanding of their risks, and how to mitigate against, and recover from cyber incidents – this is now fundamental to business risk management and potential survival.*
>
> *– ASIC Commissioner John Price*

Key contacts

For more information on the current data retention and/or de-identification and destruction requirements applicable to your organisation, as well as assistance in how best to implement the steps outlined in this guide, please contact one of our team.

Valeska Bloch
Partner, Head of Cyber
T +61 2 9230 4030
Valeska.Bloch@allens.com.au

Gavin Smith
Partner
T +61 2 9230 4891
Gavin.Smith@allens.com.au

David Rountree
Partner
T +61 7 3334 3368
David.Rountree@allens.com.au

Phil O'Sullivan
Partner
T +61 2 9230 4393
Phil.O'Sullivan@allens.com.au

Jessica Mottau
Partner
T +61 2 9230 4587
Jessica.Mottau@allens.com.au

Alex Mason
Partner
T +61 2 9230 4456
Alexandra.Mason@allens.com.au

Isabelle Guyot
Managing Associate
T +61 2 9230 4752
Isabelle.Guyot@allens.com.au