Privacy and public data:
Managing re-identification risk

Public data supports transparent and accountable government. De-identification may allow agencies to maximise the information they proactively release on public platforms.

However, agencies that publish de-identified data need to manage re-identification risks the same way they manage risks in other activities. If public data is re-identified, it can have serious consequences for stakeholders, clients and staff. *(View the Privacy and Public Data audit report.)*

Governing de-identified public data

Agencies should effectively govern de-identified public data. They should:

- know what de-identified data they publish and who is responsible for it
- have a structured end-to-end process for releasing de-identified data
- provide sufficient guidance to decision-makers who release de-identified data

Releasing de-identified public data

De-identification is technically complex and involves more than just removing names from data. Agencies should:

- fully understand their data and consider the wider risk environment
- identify and assess the risk of re-identification for each dataset
- apply appropriate treatments to reduce re-identification risk to an acceptable level

Managing re-identification risks

Re-identification risk management should be an ongoing process. Agencies should:

- regularly assess the effectiveness of existing risk treatments
- monitor the external data environment
- regularly review re-identification risks and update treatments where necessary

Office of the Information Commissioner
Queensland