JUTA
POPIA PORTAL

ISSUE NO 25 • MORE ABOUT ... INFORMATION MATCHING PROGRAMMES • MARCH 2024

MORE ABOUT ... INFORMATION MATCHING PROGRAMMES

1. OVERVIEW

To get a POPIA code of conduct accredited, a POPIA code of conduct must specify appropriate measures for information matching programmes if such programmes are used within the specific relevant sector. This article discusses different types of 'appropriate measures' a POPIA code of conduct could specify for this purpose.

Photo: iStock

2. WHAT IS AN INFORMATION MATCHING PROGRAMME?

Photo: stock.adobe.com

Firstly, what is an information matching programme? Section 1 of POPIA defines an information matching programme as follows:

> *[M]eans the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject.*

3. WHAT TYPES OF INFORMATION MATCHING PROGRAMMES EXIST?

Photo: Pexels - Ekaterina Bolovtsova

POPIA distinguishes quite clearly between information matching programmes provided for in legislation (which are dealt with in terms of sections 40(1)(*b*)(ix)(bb)and 44(2)(*a*)(i) of POPIA) and information matching programmes provided for in codes of conduct (which are dealt with in terms of section 60(4)(*a*)(i) of POPIA). An example of an information matching programme provided in a code of conduct is the example in the Banking Association of South Africa's POPIA Code of Conduct. Section 14 of this POPIA Code of Conduct provides:

> *We make use of information matching programmes to comply with the Financial Intelligence Centre Act 38 of 2001 ('FICA'). Member banks are required to conduct customer due diligence ('CDD'), on their customers and screen customers against watch lists, in accordance with their risk management and compliance programme, which governs the manner in which the member banks will comply with their obligations as set out in FICA. A bank may request the assistance of another bank to provide it with CDD information and/or documentation in relation to shared customers for the purposes of establishing and verifying the identity of the customers.*

For additional examples of different types of information matching programmes used by public bodies, you can look at this list provided by the New Zealand Government concerning immigration. New Zealand's data privacy laws also deal with information matching programmes like POPIA, so these are good examples to look at.

4. WHAT 'APPROPRIATE MEASURES' FOR INFORMATION MATCHING PROGRAMMES SHOULD YOU SPECIFY?

Photo: stock.adobe.com

Like POPIA, jurisdictions such as New Zealand and Canada make provision for 'information matching', 'data matching' or 'data linking' programmes in their data privacy legislation. Canada's legislation provides an excellent guide for what 'appropriate measures' to implement to mitigate data privacy risks provided by an information matching programme. Each Canadian province has its own respective privacy law and information and privacy commissioner. The Canadian province of Saskatchewan wrote an excellent white paper recommending certain safeguards be legislated for all data matching activities in that province. The relevant safeguards recommended here include that a data matching programme could not begin without the following:

- a privacy impact assessment being conducted;
- the purpose and scope of the programme being clearly defined; and
- everything being documented in an agreement.

Additionally, the Saskatchewan Information and Privacy Commissioner also recommended other safeguards such as:

- Organisations participating in the data matching programme should consider if the purpose of a data matching programme can be achieved using de-identified information. If so, then only de-identified information should be used.
- Data subjects whose personal information is being used in data matching programmes should be notified of this fact and be able to access the information which is being used. For example, organisations must post information about any data matching programmes they are running on their websites.
- Organisations must compile a report about any data matching programmes they run and submit this to the Information and Privacy Commissioner.
- All new personal information generated from a data matching programme must ultimately be destroyed.

Further, the ICO (the UK's Information Regulation) recommends in their 'Data Sharing: A Code of Practice' that all organisations participating in information matching or data pooling activities should conduct an accountability assessment before the information matching activity begins and document all data privacy responsibilities of all parties involved in an agreement respectively.

6. FURTHER READING

Pexels - Gül Işık

You can read more about information matching programmes in **Chapter 13.**