

# READY TO BECOME A DATA RECIPIENT?

Make sure you have these five things ready first.

## ○ DO YOU HAVE A CLEAR STRATEGY OF HOW THE BUSINESS OR ORGANISATION INTENDS TO USE THIS OPEN BANKING DATA AND WHAT IT HOPES TO ACHIEVE BY ACCESSING IT?

Several things to consider are:

- How will you be using data to develop new features or services, or enhance existing ones? Examples could include, account aggregation services and personal finance insights
- How will you improve your current data security, including existing data-sharing practices with data holders?
- Businesses need to ensure they understand how the open banking data can be used and shared, then communicate any potential changes or affects this may have on certain parties e.g. suppliers, customers, staff.
- Do you currently have the skills, resources and know-how to implement this strategy?
- Businesses need to have a plan as to how they will effectively implement new infrastructure, technologies and people to manage both the opportunities and risks housing and using the data may pose.

## ○ ARE YOU SURE YOU KNOW THE INS AND OUTS OF THE CDR RULES AND YOUR OBLIGATIONS?

Data privacy and information security is a key concern of both government and consumers. With multiple government agencies involved in the Open Banking Scheme including the ACCC, OAIC and Data Standards Body, it is important that you have an in-depth understanding of the different rules, relevant legislation and their interpretation to ensure you are compliant.

Therefore, we recommend that potential Accredited Data Recipients seek expert advice regarding their ongoing compliance obligations as well as understand the consequences of breaches.

## ○ DO YOU HAVE THE RIGHT PROCESSES, POLICIES AND CONTROLS IN PLACE FOR DATA PROTECTION AND PRIVACY IN PLACE?

The CDR has core privacy safeguards that businesses need to comply with including:

- Being able to demonstrate your control environment
- A Type I (e.g. a FinTech) ASAE 3150 accreditation standard for non-ADIs
- Compliance with relevant Privacy Safeguards and Australian Privacy principles detailed in the [CDR Privacy Safeguard Guidelines](#).

As these safeguards, principles and their applications in the CDR context can vary for different CDR entity types, businesses need to ensure they aware of these nuances and when in doubt seek advice. At BDO, our experts can assist with the above as well as providing independent accreditation, control environments, risk assessment and testing and more.





○ **DO YOU UNDERSTAND THE RELEVANT TECHNICAL STANDARDS THAT HAVE BEEN RELEASED TO ENABLE THE CDR AND HOW THEY APPLY TO YOUR BUSINESS AND CDR ENTITY TYPE?**

These include:

- Information Security profile standards
- [Consumer experience \(CX\) standards](#)
- APIs and schemas.

○ **DO YOU HAVE THE RIGHT PEOPLE AND CAPABILITY TO EFFECTIVELY IMPLEMENT THE STANDARDS INTO YOUR SYSTEMS, PROCESSES AND APPLICATIONS?**

Some key issues businesses should consider are:

- How are you ensuring a high-quality experience for consumers?
- How will ensure that the appropriate consent is obtained from consumers for any use of their data?
  - What is your process for how consent can be withdrawn and consumers can request data deletion?
  - Do you have an avenue for consumers to seek help or enquire about their data?
- What policies and procedures will you have in place regarding how data will be used and protected?

Businesses should also consider:

- How long will data be collected for (or if it is a one-off)?
- How long will the data be held?
- When and how the data will be disposed of?
- What will the impact be on your third-party relationships?
- How will you communicate these policies and procedures with consumers and ensure this information is freely available and accessible?

At BDO, we can guide you through the CDR accreditation process as well as ensure you continue to meet any ongoing obligations. Together our teams of technology, risk, forensic and audit experts can ensure you have the rights systems and controls in place to mitigate potential risks allowing your business to reap the full benefits of the Open Banking Scheme.

Should you have questions or concerns regarding the above or the CDR and your business, we encourage you to contact your local office to find out more.

## **MORE INFORMATION**

**1300 138 991 | [www.bdo.com.au](http://www.bdo.com.au)**

NEW SOUTH WALES • NORTHERN TERRITORY •  
QUEENSLAND • SOUTH AUSTRALIA • TASMANIA •  
VICTORIA • WESTERN AUSTRALIA

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact the BDO member firms in Australia to discuss these matters in the context of your particular circumstances. BDO Australia Ltd and each BDO member firm in Australia, their partners and/or directors, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO Services Pty Ltd ABN 45 134 242 434 is a member of a national association of independent entities which are all members of BDO Australia Ltd ABN 77 050 110 275, an Australian company limited by guarantee. BDO Services Pty Ltd and BDO Australia Ltd are members of BDO International Ltd, a UK company limited by guarantee, and form part of the international BDO network of independent member firms. Liability limited by a scheme approved under Professional Standards Legislation.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© 2020 BDO Services Pty Ltd. All rights reserved. FS 20-024