Cowell Clarke
COMMERCIAL LAWYERS

FS Compliance Newsletter

OCTOBER 2026

Contents

Introduction 1

Regulation 2

Consultation 5

AUSTRAC 6

New privacy obligations for automated decision-making 8

Get in touch with our team 10

Disclaimer: This publication has been prepared for general guidance on matters of interest only and does not constitute professional legal advice. You should not act upon the information contained in this publication without obtaining specific professional legal advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication and to the extent permitted by law, Cowell Clarke does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting or refraining to act in relation on the information contained in this publication or for any decision based on it.



Introduction

In this edition, ASIC reports that the private credit industry continues to present issues relating to opaque fee structures, inconsistent reporting, weak governance and poor valuation practices. ASIC has also issued a warning to AFS licensees regarding their use of lead generation services.

ASIC announced that it is commencing a further review of the Financial Advisers Register and has also released a report highlighting significant shortcomings in how superannuation trustees manage and learn from member complaints, urging trustees to review their practices without delay. ASIC is also seeking feedback on a proposal to extend the existing tax advice exemption for licensees in *Instrument 2016/1151*.

Furthermore, ASIC has commenced a consultation on the implementation of the *Corporations Amendment (Digital Assets Framework) Act 2026*, which will introduce a new regulatory regime for digital asset platforms and tokenised custody platforms, representing a significant development in Australia's approach to digital asset regulation.

AUSTRAC continues to release guidance material to assist reporting entities in meeting their anti-money laundering and counter-terrorism financing obligations, focusing on compliance fundamentals, effective customer due diligence and timely reporting.

Regulation

ASIC continues its surveillance of private credit funds and highlights ongoing concerns

On 10 November 2026, ASIC released Report 846 *Private credit funds: Do investors know what they're getting?* (**REP 846**) outlining observations from its further additional surveillance of the private credit industry, finding that many of the previous concerns with opaque fee structures, inconsistent reporting, weak governance and poor valuation practices remain.

REP 846 is based on a review of 24 wholesale and retail private credit funds over a nine-month period between November 2025 and August 2026. It follows earlier ASIC reviews that resulted in Report 814 Private credit in Australia and Report 820 *Private credit surveillance: retail and wholesale funds*.

While ASIC observed some industry improvement, its recent surveillance found that many investors continued to receive inadequate information to allow them to make informed investment decisions about whether to invest in the fund.

REP 846 identified continued shortcomings, including:

- complex structures and arrangements that masked conflicts and fees;
- incomplete or inconsistent fee disclosure, including failing to clearly disclose when fees were being retained by fund managers; and
- retail distribution practices that failed to clearly communicate risks and support informed decision making.
- higher concentrations of investor funds showed an increased likelihood that financial advisers could not demonstrate compliance with the best interests duty.

The surveillance has already resulted in six interim stop orders and multiple referrals for enforcement investigation.

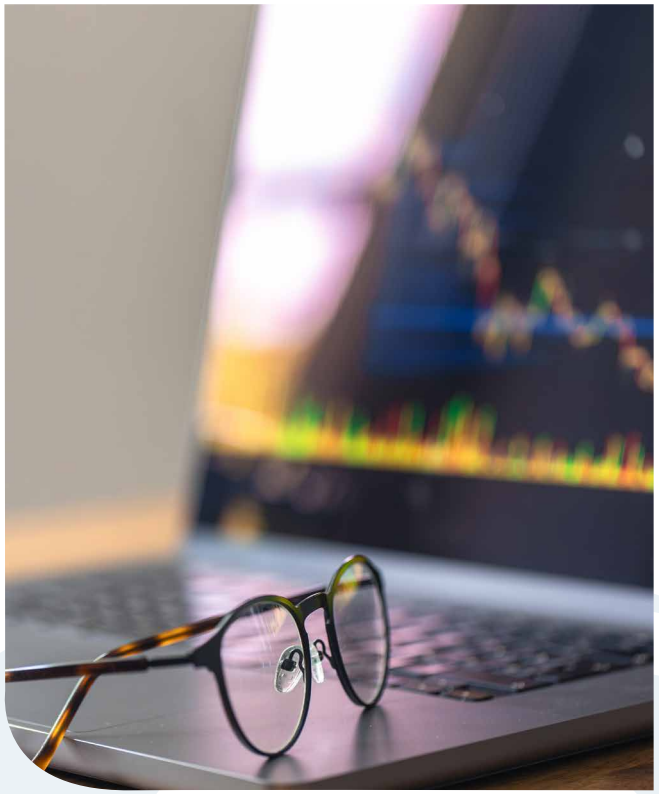
ASIC set its expectations to fund operators, distributors, intermediaries and financial advisers to carefully consider the findings in the report and embed its ten principles of private credit done well into practice. ASIC made it clear in its report that "It is not acceptable for funds to wait until there is regulator engagement to improve practices. Poor private credit practices is an enforcement priority for ASIC and ASIC will take action where required".

For reference the ten principles of private credit done well are:

1. **Stewards of other people's money** - Fund operators act as stewards of investor capital, ensuring that their decisions are fair and in investors' best interests.
2. **Organisational capability** - Human, financial and technological resources are adequate. Fund operators operate efficiently, honestly and fairly.
3. **Transparency** - Investors have access to timely, transparent information on investment strategy, exposures, valuations, risks and fees.
4. **Design and distribution** - Design and distribution practices are fair, transparent and appropriately targeted for investors.
5. **Fees and costs** - Fees and costs are fair and transparent, giving investors and borrowers a clear view of total costs.
6. **Conflicts of interest** - Conflicts of interest are identified, disclosed and effectively managed or avoided.
7. **Governance** - Structures, processes and people promote sound decision-making, compliance and accountability.
8. **Valuations** - Valuations are fair, timely and transparent, with robust governance.
9. **Liquidity** - Liquidity risk is effectively disclosed and managed, avoiding structural mismatches, with fair redemption terms aligned to portfolio liquidity.
10. **Credit risk** - Credit risk is effectively managed across loan origination, portfolio construction, monitoring, impairment, default and repayment.

We recommend that fund managers and financial advisers closely scrutinise the results of **REP 846** and consider their own practices in respect of private credit funds in particular but also fund practices more broadly.

The full media release can be viewed here.



Lead generation under scrutiny: ASIC issues final warning to advice licensees

On 9 November 2026, ASIC issued *Report 845 Lead generation advice models: Putting consumers and licensees at risk* (**REP 845**) and in doing so issued a final warning to AFS licensees about their use of lead generators after finding that inadequate licensee oversight has exposed consumers to unacceptable risk of harm.

REP 845 draws on an 18-month surveillance of 15 licensees, finding that weaknesses in licensee oversight have enabled lead generators to perform roles they are neither licensed for nor qualified to undertake.

REP 845 found that lead generators were:

- completing specialist tasks, including conducting fact-finds, assessing clients' risk profiles, and discussing advice recommendations with clients; and
- using potentially misleading statements and fear-based claims to encourage consumers to review their superannuation and switching investments.

These findings highlight serious shortcomings in how licensees monitor lead generators' interactions with clients. ASIC Commissioner Alan Kirkland emphasises that "the findings in [REP 845] sends a clear warning to advice licensees that using or allowing lead generation services may put their licenses at risk."

Clients sourced through lead generation accounted for 35% of all new clients received by the businesses under surveillance. Over the 18-month period, these clients generated $9.8 million in initial fees for the advice businesses of the 15 participating licensees, as well as commitments to a further $4.3 million in ongoing fees.

Proposed reforms targeting lead generation

The recent failures of Shield and First Guardian Master Fund, alongside broader losses in the self-managed superannuation sector, highlight why ASIC considers preventative measures essential.

On 19 August, government reforms were released to strengthen protections for Australian consumers within the superannuation and financial system. Part of these reforms specifically target risks associated with the lead generation sector, including:

- banning unlicensed real-time communication with consumers about superannuation, with targeted exemptions for advocacy, educational and employment communications;
- enhancing the consent requirements for real-time contact with consumers;
- strengthening anti-hawking protections to support more timely and scalable regulatory action, while protecting low-risk arrangements;
- requiring licensees to take reasonable steps to ensure lead generation activities are undertaken in compliance with relevant regulatory and legal requirements; and
- undertaking further targeted consultation to determine potential high-risk forms of lead generation and consumer harm.

The full media release can be viewed here.

ASIC continues review of Financial Advisers Register records

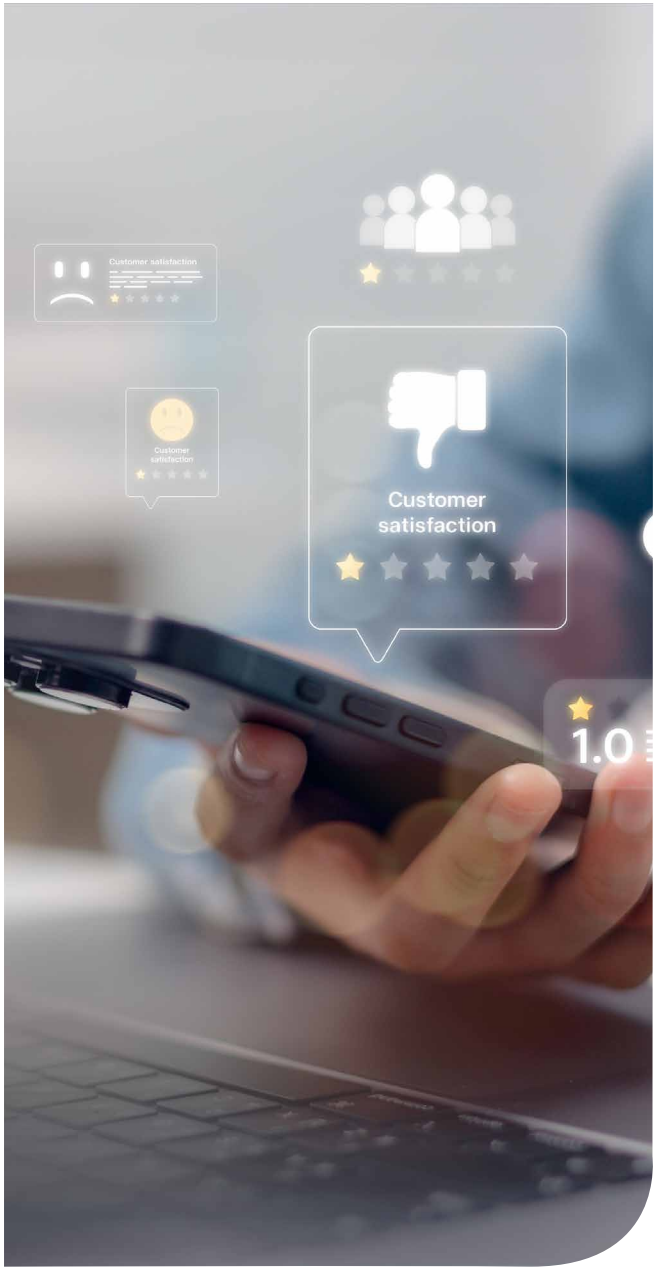
ASIC announced on 30 October 2026, that it has commenced a further review of the Financial Advisers Register (**FAR**) records. This review will examine whether a sample of qualifications and training courses recorded by Australian financial services licensees as contributing towards their relevant providers meeting the qualifications standard.

This follows ASIC's initial review in February 2026, which examined relevant providers whose FAR records did not include any qualifications or courses as going toward meeting the qualifications standard. The qualifications standard commenced on 1 January 2026. As a result of that review, 26 relevant providers had their authorisation to give personal advice to retail clients on relevant financial products ceased.

ASIC continues to monitor notifications about relevant providers relying on the experienced provider pathway to meet the standard.

The full media release can be viewed here.





ASIC calls out superannuation trustees for significant deficiencies in managing member complaints

On 2 November, 2026 ASIC published *Report 844 – Lessons to be learned: How trustees use insights from superannuation complaints* (**Report 844**), which revealed that many trustees are failing to use complaints as early warning signs of systemic issues. ASIC has characterised the findings as a significant industry-wide concern, noting that these practices can breach obligations, cause harm to members and undermine confidence in the superannuation system.

In Report 844, ASIC highlighted several interconnected issues contributing to inadequacies in trustees' processes to identify and respond to systemic issues from complaints:

- Insufficient trustee diligence in meeting obligations under Regulatory Guide 271: Internal Dispute Resolution (RG-271).
- Low rates of systemic issue identification.
- A lack of customer focus. This extends to trustees too readily attributing the root cause of complaints to members and a lack of learning from significant transformational changes.
- Inadequate governance arrangements.
- Gaps in complaints data capture and analysis.

Key takeaways for superannuation trustees

ASIC has urged all trustees to review Report 844 without delay and assess the adequacy of their IDR arrangements to identify and respond to systemic issues. If necessary, ASIC has encouraged trustees to seek external assistance in meeting their obligations.

Supporting better retirement outcomes and superannuation member services is a strategic priority for ASIC, as stated in its 2026/27 Corporate Plan. It has advised it will continue to monitor industry practices and will consider "the full range of regulatory responses available" where members are exposed to harm because trustees failed to address weaknesses. ASIC has already taken legal action against a number of trustees for contraventions of their systemic issue management or internal dispute resolution (IDR) obligations.

Refer to ASIC REP-844 here.

The full media release can be viewed here.

ASIC proposes to continue tax advice exemption in Instrument 2016/1151

ASIC is seeking feedback on a proposal to extend an existing tax advice exemption for licensees for a further five years. The exemption in *ASIC Corporations (Recognised Accountants: Exempt Services) Instrument 2016/1151* is due to expire on 1 April 2027, however ASIC believes that the exemption remains useful and necessary. It plans to remake the instrument with minor updates with no change to its effect.

Submissions should be sent to rri.consultation@asic.gov.au by 5pm AEST 25 November 2026.

Refer to CS 67 Proposed remake of instrument allowing limited exempt tax advice.

The full media release can be viewed here.

Consultation

ASIC consults on implementation of new digital asset laws

On 15 October 2026, ASIC released Consultation Paper *392 Digital asset law reform implementation: Proposed standards and guidance* (**CP 392**). CP 392 is particularly significant because it provides the first detailed indication of how ASIC intends to administer Australia's new digital asset regulatory regime established by the Digital Assets Framework (**DAF**) Act. While the DAF Act establishes the legislative framework, CP 392 outlines the preliminary draft standards, proposed modifications and relief under the Corporations Act, and draft regulatory guidance regarding the implementation of the regime, which will commence on 8 April 2027.

The DAF Act is an important reform to Australia's financial services regulatory framework. It will expand Australia's financial services licensing regime to regulate entities providing services in relation to financial products Digital Assets Platforms (**DAPs**) and Tokenised Custody Platforms (**TCPs**). The reforms are intended to address regulatory gaps, provide greater certainty for businesses, investors and consumers and align Australia's financial regulation frameworks with comparable overseas jurisdictions.

ASIC seeks feedback in relation to the following proposals relating to DAPs and TCPs:

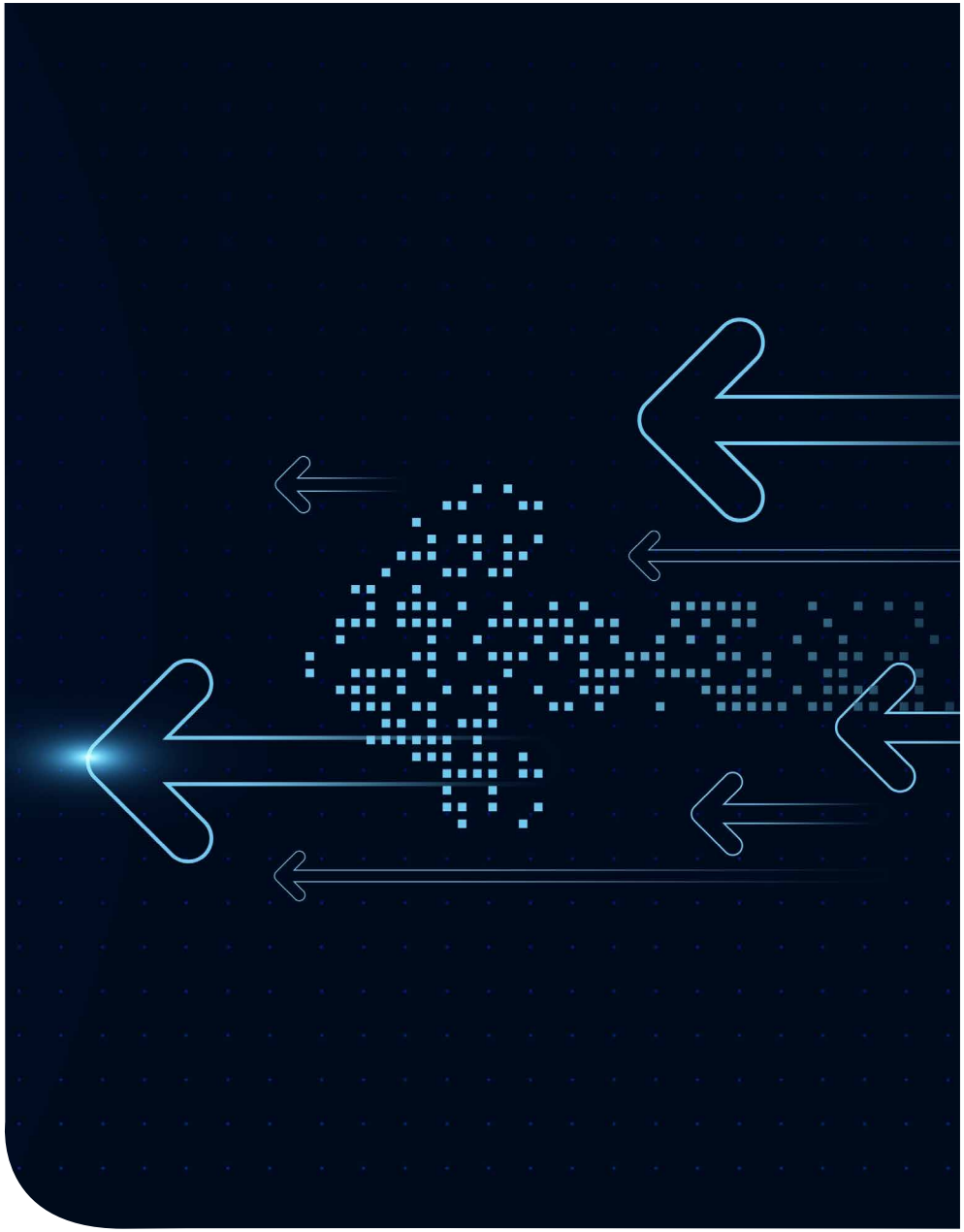
- Regulatory guidance relating to DAPs and TCPs;
- Asset-holding standards;
- Transactional and settlement standards; and
- Financial requirements for DAP and TCP licensees.

If you are currently operating a platform that will be considered a DAP or TCP on 8 April 2027, you must apply for an Australian financial services licence or variation by 7 October 2027.

Consultation closes at 5pm on 27 November 2026.

The email address for submissions is fintech@asic.gov.au.

The full media release can be viewed here.



AUSTRAC

Upcoming Changes to the AML/CTF Act

On 16 November 2026, the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026* (**Amendment Bill**) passed both Houses of Parliament. The Amendment Bill will become law when it receives the Royal Assent, which can take up to 10 business days.

Relevantly, the Amendment Bill makes the following changes to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (**AML/CTF Act**):

1. You will no longer be required to establish on reasonable grounds whether a person acting on behalf of the customer (i.e. an **agent** of the customer) is a politically exposed person.
2. You will no longer be required to complete enhanced customer due diligence on a customer where an agent of the customer is a foreign politically exposed person.
3. Changes will be made to the definitions of 'domestic politically exposed person' and 'foreign politically exposed person', to clarify the application of these definitions where a reporting entity provides designated services at or through a permanent establishment of the reporting entity in a foreign country.
4. These changes will commence the day after the Amendment Bill receives the Royal Assent.

In response to the above changes, material updates to AUSTRAC's regulatory guidance and observed industry practice over the past 8 months, AML/CTF Program's should be updated to:

a. reflect the upcoming changes to the AML/CTF Act;
b. improve your AML/CTF Program based on material updates to AUSTRAC's regulatory guidance (including removing unnecessary requirements, clarifying relevant processes, and providing helpful examples), ensuring that you are meeting AUSTRAC's latest expectations; and
c. simplify and streamline your AML/CTF Program based on observed industry practice, giving you more flexibility and reducing your compliance burden.

Please get in touch with our financial services team to discuss changes to your AML/CTF Program to reflect the above.



Five fundamentals for AML/CTF compliance

On 30 September, AUSTRAC provided five tips to support regulated businesses to comply with their AML/CTF obligations at a fundamental level. These recommendations follow updates to AML/CTF legislation which took effect in March and July 2026.

The five recommendations are:

1. Businesses must understand which requirements apply to their specific business to focus attention appropriately and avoid unnecessary expenditure on compliance measures that do not apply to the business.
2. AUSTRAC Online details must remain up to date to avoid missing important information about obligations, regulatory changes and guidance.
3. Businesses should know their risks and implement mitigating controls against criminal exploitation. Risks should be reviewed regularly, when a business launches new service offerings or engages with new client groups.
4. Execute reporting obligations correctly. Reporting enables law enforcement to understand criminal activity, particularly when reviewed together with information from other reporting entities.
5. Maintain accurate and organised records to support compliance with AML/CTF obligations and facilitate risk identification.

The full media release provides links to helpful resources throughout the article and can be viewed here.



Effective customer due diligence

On 30 September, AUSTRAC published a media release in respect of customer due diligence (**CDD**). CDD involves collecting and verifying a customer's information to manage money laundering and terrorism (**ML/TF**) financing risks. CDD is essential in fulfilling the AML/CTF 'know your customer' (**KYC**) obligations.

KYC involves:

- Identifying your customers;
- Checking their identity;
- Understanding who may be acting on their behalf; and
- Understanding any risks they may present.

CDD may involve:

- Requesting customer identification when opening an account, starting a service or completing certain transactions.
- Requesting additional information, such as the purpose of a transaction.
- Assessing the risk level of a customer based on circumstantial factors.
- Imposing additional verification or monitoring requirements if a customer poses an increased level of risk.

Effective CDD will enable a business to know their customer's identity, understand who owns and controls their customer and identify any risks or suspicious activity. CDD continues after onboarding a customer. A customer's risk profile can change over time. Regular reviews of customer risk profiles are an encouraged CDD practice.

The full media release can be viewed here.

Timely reporting

AUSTRAC has also reminded businesses in a media release published 30 September 2026, that accurate and timely reporting provides critical intelligence for law enforcement agencies, enabling them to protect against money laundering, terrorism financing and other serious crime. Reporting is conducted through three report types.

Threshold transaction reports (**TTR**) must be submitted:

- When a business provides a designated service involving the transfer of $10,000 or more (Australian currency or a foreign currency equivalent) in physical currency.
- Within 10 days of the transaction.

Suspicious matter reports (**SMR**) must be submitted:

- If there are reasonable grounds to suspect a matter covered by AML/CTF legislation.
- Within 24 hours of a suspicion forming if it relates to terrorism financing.
- Within 3 business days for any other type of suspicion.

Annual compliance reports demonstrate how a business met its AML/CTF obligations during the previous financial year. The next annual compliance report will cover activities during the 2026-2027 financial year and must be lodged between 1 July 2027 and 30 September 2027.

AUSTRAC acknowledged that some entities are newly regulated and therefore are not expected to report perfectly, but should demonstrate that their AML/CTF program is being followed.

The full media release can be viewed here.

New privacy obligations for automated decision-making

From **10 December 2026**, 'APP entities' regulated under the Privacy Act (which include 'reporting entities' regulated under the AML/CTF Act) must disclose certain information in their Privacy Policies where they have arranged for a computer program to make or inform decisions that significantly affect individuals' rights or interests. This is referred to as the "transparency obligation".

When does the transparency obligation apply?

The transparency obligation will apply where:

1. you have arranged for a computer program to make a decision, or to do a thing that is substantially and directly related to making a decision; and
2. the decision could reasonably be expected to significantly affect the rights or interests of an individual; and
3. personal information about the individual is used in the operation of the computer program to make the decision or do the thing that is substantially and directly related to making the decision.

What is a computer program?

The concept of a 'computer program' is quite broad, including not only artificial intelligence (AI) but also everyday software and applications, such as formulas in spreadsheets.

When is something substantially and directly related to making a decision?

Something will be 'substantially' related to making a decision where it is a key factor in facilitating the human's decision making.

Something will be 'directly' related to making a decision where it has a direct connection with making the decision.

For example, a computer program may be substantially and directly related to making a decision if it:

- determines the outcome of a process; or
- advises of an appropriate outcome of a process; or
- in any way influences the outcome of a process.

As provided by the Office of the Australian Information Commissioner (OAIC):

"A computer program may be substantially and directly related to making a decision regardless of whether the nature of the output is advisory or determinative. In this regard, the OAIC considers machine learning or generative AI outputs used to make decisions that significantly affect the rights or interests of individuals would generally fall within the scope of the transparency obligation unless subject to extensive human oversight and control." (emphasis added)

That is – just because a human reviews the computer program's output, does not mean that it is out of scope of the transparency obligation.

When will a decision significantly affect the rights or interests of an individual?

To 'significantly' affect the rights or interests of an individual, the impact of the decision must be more than trivial and must have the potential to considerably influence the circumstances or outcomes for the individual concerned.

What are some examples of decisions that would generally be considered in scope of the transparency obligation?

The OAIC provides the following non-exhaustive list of examples of decisions that would generally be considered in scope of the transparency obligation:

- facial recognition technology use in a retail store or stadium for watchlist matching;

New privacy obligations for automated decision-making (con't)

- recruitment software used to sort through candidate profiles and make hiring decisions;
- differential and/or personalised pricing practices used by online retailers in the sale of significant goods;
- computer programs used to prioritise the provision of health or disability services to individuals;
- computer programs which determine eligibility for the provision of a government benefit or housing assistance;
- computer programs which determine eligibility for admission to an education or training program;
- computer programs used to approve or reject a loan or credit application;
- programmatic advertising relating to the decision to sell significant goods or services;
- computer programs involved in assessing an individual's eligibility for insurance;
- reports created by artificial intelligence used to rank employee performance, determine promotions, or decide bonus/remuneration outcomes;
- computer programs involved in decisions relating to the provision of a scholarship, grant or other financial support;
- computer programs used to process immigration applications or enforce border controls at an airport.

We consider that another example may be where a reporting entity uses a third-party technology solution to complete customer due diligence under the AML/CTF Act. If you use a third-party technology solution to complete customer due diligence under the AML/CTF Act, we recommend that you:

1. inquire with the vendor of the solution as to whether or not the solution will fall within the scope of the transparency obligation; and
2. if so – request that the vendor of the solution provide you with the information that you will need to update your Privacy Policy.

What information must be disclosed?

Where the transparency obligation applies, you must disclose the following information in your Privacy Policy:

1. the kinds of personal information used in the operation of such computer programs; and
2. the kinds of such decisions made solely by the operation of such computer programs; and
3. the kinds of such decisions for which a thing, that is substantially and directly related to making the decision, is done by the operation of such computer programs.

Next steps

Licensees should complete a comprehensive review of the computer programs that they use in their business to make, or help them make, decisions (including third-party software and applications). For example: computer programs that help to determine whether or not an investor is eligible for a financial product based on the investor's completion of an online questionnaire; computer programs that calculate a client's risk profile based on the client's answers to specific questions; or computer programs that recommend suitable financial products for a person based on their relevant personal circumstances. Licensees should then assess whether or not their use of these computer programs will be subject to the transparency obligation and, if so, update their Privacy Policy before 10 December 2026.

For more information, please refer to the OAIC's *Transparency Obligation Fact Sheet* link.

If you are concerned that your use of a computer program may fall within scope of the transparency obligation, please get in touch with Cowell Clarke's Financial Services Team at Compliance@CowellClarke.com.au.

Get in touch with our team



Richard Beissel
Director
D: +61 8 8228 1140
E: rbeissel@cowellclarke.com.au



Mayank Gupta
Director
D: +61 2 8255 6907
E: mgupta@cowellclarke.com.au



Emma Johnson
Senior Associate
D: +61 2 8255 6910
E: ejohnson@cowellclarke.com.au



Andrew Mutton
Senior Advisor
D: +61 2 8255 6927
E: amutton@cowellclarke.com.au



Zac Mizgalski
Associate
D: +61 8 8228 1123
E: zmizgalski@cowellclarke.com.au



Barbara Vrettos
Senior Associate
D: +61 2 8255 6939
E: bvrettos@cowellclarke.com.au



Monique Micklethwaite
Compliance Services Manager
D: +61 8 8228 1121
E: mmicklethwaite@cowellclarke.com.au



Rhea Bhargava
Lawyer
D: +61 8 8255 6963
E: rbhargava@cowellclarke.com.au



Chloe Kowalczuk
Client Growth Manager
D: +61 8 8228 1176
E: ckowalczuk@cowellclarke.com.au

Email our team with your financial services queries or about our AFSL Compliance Support

CLICK HERE

