EXPLANATORY STATEMENT

Approved by the Australian Communications and Media Authority

Telecommunications Act

Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025

Authority

The Australian Communications and Media Authority (the **ACMA**) has made the *Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025* (the **Standard**) under subsection 125AA(1) of the *Telecommunications act 1997* (the **Act**) and in accordance with sections 5, 6 and 7 of the *Telecommunications (Domestic, Family and Sexual Violence Consumer Protections Industry Standard) Direction 2024* (the **Direction**).

Under subsection 125AA(4) of the Act, the Minister for Communications (the **Minister**) has the power to direct the ACMA to:

(a) determine a standard under subsection 125AA(1) of the Act that:

  (i) applies to participants in a specified section of the telecommunications industry;

  (ii) deals with one or more specified matters relating to the activities of those participants; and

(b) do so within a specified period.

The Direction was given to the ACMA by the Minister under subsection 125AA(4) of the Act and commenced on 10 December 2024. It requires the ACMA to determine an industry standard under subsection 125AA(1) of the Act that deals with safeguarding telecommunications consumers who are, or may be, affected by domestic and family violence (**DFV**), and where relevant, sexual violence.

The Standard meets the requirements and objectives in sections 5, 6 and 7 of the Direction. In accordance with subsection 5(2) of the Direction the Standard was determined no later than six months after the commencement of the Direction. In accordance with paragraph 5(2)(b) of the Direction, the Standard commences at the earliest practicable opportunity which is on 1 July 2025 for some provisions and on 1 January 2026 for the remaining provisions (**the 1 January provisions**). The staggered commencement of the Standard allows for telecommunications providers to have sufficient time to prepare for the implementation of obligations which require consultation or the establishment of new systems and processes. Pursuant to subsection 4(2) of the Standard, small providers are given 3 months extra to implement the 1 January provisions, which will apply to small providers from 1 April 2026.

Purpose and operation of the instrument

Background

Domestic, family and sexual violence (**DFSV**) causes profound harm across Australian society. One in four women and one in eight men have experienced violence by an intimate partner or family member since the age of 15. Intimate partner violence is the leading risk factor contributing to illness, disability, and premature death for women aged 25–44. Certain groups, including younger women, Aboriginal or Torres Strait Islander people, and people living with a disability are disproportionately affected.

The *National Plan to End Violence against Women and Children 2022-2032* (**the National Plan**) is the Australian Government's overarching strategy to end gender-based violence within one

generation. The National Plan recognises that addressing violence against women and children requires a whole-of-community approach, with businesses and the corporate sector playing a vital role.

Telecommunications services are essential for participation in modern life, enabling access to employment, education, healthcare, banking, government and community support. For victim-survivors of DFSV, access to safe, reliable and secure communications can be critical to safety, privacy and wellbeing. Telecommunications services play a vital role in supporting victim-survivors to stay connected, seek help and plan for safety. Conversely, communications can also be used to compromise safety and security and facilitate DFV, for example via technology facilitated abuse and/or economic abuse.

Although the industry developed a voluntary guideline (Communications Alliance G660:2023 Assisting Consumers Affected by Domestic and Family Violence), a need has been recognised for an enforceable regulatory instrument requiring minimum, consistent protections for consumers affected by DFSV across the telecommunications sector. While some providers have taken steps to adopt practices that support affected consumers, the level of uptake and implementation across the sector is unclear. Recognising the importance of this issue, the Australian Government determined that enforceable obligations are necessary so that all consumers affected by DFSV receive appropriate support from their telecommunications provider. The Minister's Direction acknowledges the essential role the telecommunications sector plays in safeguarding victim-survivors and supporting their rights to privacy, safety and ongoing connectivity.

Purpose

The purpose of the Standard is to ensure that carriers and carriage service providers (**CSPs**) take effective, timely and trauma-informed action to support telecommunications consumers who are, or may be, affected by domestic and family violence, and where relevant, sexual violence.

The Standard gives effect to the objectives set out in the Direction by:

- requiring CSPs to take action to protect the safety and security of affected consumers;
- ensuring CSPs maintain the privacy of personal information and the security of telecommunications accounts;
- mandating personnel training and internal support structures to enable appropriate identification of, and responses to, affected consumers;
- promoting the development and implementation of policies and processes that account for the needs of diverse and disproportionately affected consumer groups;
- requiring CSPs to provide prompt and appropriate assistance to support affected consumers to remain safely connected to telecommunications services;
- reducing the risk of harm by identifying and addressing risks within telecommunications systems, processes and products;
- limiting the disclosure of information in customer-facing communications that may compromise a consumer's safety;
- promoting consumer awareness of available assistance and referrals to specialist support services;
- requiring CSPs to maintain relevant records and demonstrate compliance with the Standard; and
- encouraging CSPs to consider safe and appropriate practices for staff in engaging with alleged perpetrators of DFSV.

Operation

The Standard has been made to fulfil the requirements of the Direction. It establishes enforceable consumer protections that apply to telecommunications providers dealing with consumers who are, or may be, affected by domestic, family or sexual violence.

Part 1 sets out the name, commencement date and application of the Standard. It includes definitions of key terms used throughout the instrument, and sets out to whom the Standard applies. The Standard applies to CSPs that deal with residential, small business and not-for-profit (**NFP**) consumers, as well as to carriers in relation to their supply of carriage services to CSPs.

Part 2 requires that where a consumer seeking support with their telecommunications products discloses that they have experienced sexual violence outside of a DFV situation, the CSP must treat the consumer as an affected person for the purposes of providing telecommunications support in accordance with specified provisions of the Standard.

Part 3 sets out the advice and support that a CSP must offer an affected person. It includes minimum requirements about what information must be given to an affected person, when and how to communicate with them and the minimum support that must be offered.

Part 4 requires that a CSP must publish a DFV statement, and it sets out minimum content and accessibility requirements for the DFV statement. It also includes requirements relating to the access a CSP must give an affected person to DFV support services.

Part 5 requires CSPs to establish and comply with a DFV policy and DFV procedures for supporting affected persons. It specifies minimum content for the policy and procedures.

Part 6 requires that CSPs must deliver appropriate DFV training for all personnel who are involved, either directly or indirectly, with consumers in Australia. It requires training on its DFV policy for these personnel, with more detailed training for customer-facing personnel, including how to engage with and respond to affected persons.

Part 7 sets out requirements for monitoring and review of the DFV policy and DFV procedures and how staff are complying with these. It imposes requirements on a CSP to take action where it identifies that the policy or procedures are not operating as intended.

Part 8 imposes minimum requirements on CSPs in relation to account security and the protection of personal information of affected persons. It includes obligations to prevent and respond to unauthorised access and misuse.

Part 9 requires CSPs to keep records to demonstrate compliance with the Standard. It also includes requirements for record retention and the disposal or destruction of specific materials.

Part 10 requires CSPs to consult with persons or bodies with DFV expertise in the development of their DFV policies, procedures and training materials. This is to support an 'inclusive design' approach and improve outcomes for affected persons.

Part 11 confers powers and functions on the Telecommunications Industry Ombudsman (**TIO**) in relation to consumer complaints about the matters covered by the Standard, in order to provide effective dispute resolution pathways for affected consumers.

A provision-by-provision description of the instrument is set out in the notes at **Attachment A**.

The Standard is a legislative instrument for the purposes of the *Legislation Act 2003* (the **LA**) and is disallowable and subject to the sunsetting provisions in Part 4 of Chapter 3 of the LA.

If a standard is contravened, the ACMA may:

> issue a formal warning

> give a remedial direction

> accept an enforceable undertaking

> give an infringement notice

> seek an injunction in the Federal Court to compel the person to act or refrain from acting in a particular way

> seek civil penalties via Federal Court proceedings (up to $50,000 for a person and $250,000 for a body corporate per contravention).

Documents incorporated by reference

Subsection 589(1) of the Act provides that an instrument under the Act may make provision in relation to a matter by applying, adopting or incorporating (with or without modifications) provisions of any Act as in force at a particular time, or as in force from time to time.

Subsection 589(2) of the Act provides that an instrument under the Act may make provision in relation to a matter by applying, adopting or incorporating (with or without modifications) matter contained in any other instrument or writing as in force or existing at a particular time, or as in force or existing from time to time, even if the other instrument or writing does not yet exist when the instrument made under the Act is made.

The Standard incorporates or refers to the following Acts and legislative instruments (including by the adoption of definitions), which are available free of charge on the Federal Register of Legislation (http://www.legislation.gov.au) (the **Register**):

- the Act
- the *Acts Interpretation Act 1901* (**AIA**)
- the *Broadcasting Services Act 1992*
- the Direction
- the LA
- the *Privacy Act 1988* (**Privacy Act**)
- the *Telecommunications (Emergency Call Service) Determination 2019*
- the *Telecommunications (Financial Hardship) Industry Standard 2024.*

The Acts and legislative instruments listed above that have been incorporated are incorporated as in force from time to time, in accordance with section 10 of the AIA, subsection 13(1) of the LA and section 589 of the Act.

The Standard also incorporates, the *C525 Handling of Life Threatening and Unwelcome Communications Industry Code.*

The *C525 Handling of Life Threatening and Unwelcome Communications Industry Code* has been incorporated as in force or existing from time to time (see subsection 589(2) of the Act) and can be accessed free of charge on Communications Alliance's website: https://www.commsalliance.com.au.

Consultation

Before the Standard was made, the ACMA was satisfied that consultation was undertaken to the extent appropriate and reasonably practicable, in accordance with section 17 of the LA and subsection 125AA(3), and sections 132, 133, 134 and 135 of the Act.

The ACMA consulted with Communications Alliance (being a body that represents the telecommunications industry), the TIO, the Australian Competition and Consumer Commission, the Office of the Australian Information Commissioner, the Australian Communications Consumer Action Network (being a body that represents the interests of consumers), industry stakeholders, consumer groups, DFV advocacy groups and the public on the making of the Standard. Between 25 February 2025 and 2 April 2025, the ACMA conducted a public consultation process, through the release of a draft Standard and a consultation paper on the ACMA's website.

On 26 February 2025, the ACMA also published a notice in *The Australian* newspaper, being a newspaper circulating nationally. It stated that the ACMA has prepared a draft Standard, advising that a copy could be accessed via the ACMA's website and inviting interested persons to give written comments by 2 April 2025.

The ACMA informed key stakeholders of the publication of the documents and invited comment on the draft of the Standard and on the issues set out in the accompanying consultation paper. The ACMA also held two online consultation workshops, one on 17 March 2025 for industry stakeholders, and the second on 24 March 2025 for DFV and consumer advocates. The ACMA also met with a number of people who have lived experience of DFV.

The consultation paper sought comment on several key issues included in the draft Standard as well as inviting general comments. The ACMA received 21 submissions from a range of stakeholders including participants in the telecommunications industry, consumer and DFV advocates, the TIO and government agencies. The ACMA considered all relevant issues raised by the submissions in the consultation process when making the Standard.

All non-confidential submissions were published on the ACMA website between 11 and 16 April 2025.

The submissions provided a broad range of feedback on the draft Standard. Key issues raised by stakeholders included the following:

- Suppression of information – industry stakeholders identified technical and feasibility issues with the application of an opt in/opt out model and the suppression of charged calls compared to zero-rated numbers. There was widespread support among all stakeholders for the list of numbers for suppression to sit outside the Standard itself and be operated by a neutral party such as the ACMA. The Standard includes 1800 numbers for relevant national services. There will be a later opportunity to propose amendments to expand the list following further inquiry into technical, operational and feasibility matters.
- Level of prescriptiveness – all stakeholders supported a flexible, consumer-led approach but there were different views on the level of specificity in the requirements that would best deliver this. Industry have argued for less prescriptive requirements, while consumer advocates consider that more specific requirements mandating what CSPs must do and offer to affected persons are needed. The Standard reflects elements of both approaches and detailed guidance will be developed to complement the application of the instrument.
- Application of the standard – consumer advocates and government stakeholders were of the view that the Standard should cover small businesses and NFP organisations and provided cases where small business consumers had or could be affected by DFV. The majority of industry stakeholders opposed extending the Standard to small businesses and NFPs due to the risks and complexities involved in transfers and authorisations with business accounts. We have included

certain small business consumers and NFP organisations in the definition of "consumer" in the Standard.

- Consultation with experts – there was broad general support for the inclusion of consultation with DFV experts in developing DFV policies, procedures and training. However, there were differing views regarding the scope and nature of such consultation and the potential burden on the DFV sector in providing advice. The Standard requires CSPs to consult with a DFV support service or organisation and one of either a panel with lived experience or an organisation representing persons disproportionately affected by DFV. It also allows industry bodies to consult on behalf of small providers.
- Interaction with other instruments –industry stakeholders raised concern about potential conflicts between the Standard and other regulations including the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022*, the *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017*, and the *Telecommunications (Financial Hardship) Industry Standard 2024*. We have included provisions in the Standard to address potential conflicts and harmonise the interaction of the protections by allowing for exemptions where the action would contravene another law or limiting the timeframe of an action so that the action does not conflict with other legislative requirements.
- Collection of evidence – we received conflicting feedback from stakeholders on this matter. Many industry participants raised concerns that an absolute prohibition on the collection of evidence may expose the providers, and consumers themselves, to the risk of fraud or systems abuse. Most consumer advocates were adamantly opposed to the collection of evidence under any circumstances, considering it can place an additional burden on someone already facing extreme stress and trauma. The Standard balances the need to manage potential exploitation by bad actors with the need to minimise barriers for affected persons by allowing for evidence to be collected where it is legally required or where it is necessary to protect the interests of a DFV affected person.
- Implementation - all stakeholders indicated a need to allow sufficient time for consultation on policies, procedures and training. There was also widespread acknowledgement that smaller providers would likely require more time for implementation although some larger CSPs posit that they require more time than smaller CSPs due to the size and complexity of processes and systems. Consumer advocates considered that many of the provisions which deal with the provision of direct support to affected persons should commence immediately, while industry noted that before support requirements could be implemented, the underlying policies, procedures, systems and training (requiring consultation) would be required. The Standard balances this feedback with a staggered approach to implementation.

Statement of compatibility with human rights

Subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* requires the rule-maker in relation to a legislative instrument to which section 42 (disallowance) of the LA applies to cause a statement of compatibility with human rights to be prepared in respect of that legislative instrument.

The statement of compatibility with human rights set out in **Attachment B** has been prepared to meet that requirement.

Attachment A

Notes to the *Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025*

Part 1–Preliminary

Section 1 Name

This section provides for the industry standard to be cited as the *Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025* (the **Standard**).

Section 2 Commencement

The obligations under the Standard commence in a staggered manner to allow telecommunications providers sufficient time to prepare for implementation, particularly where obligations require prior consultation or the establishment of new systems and processes.

This section provides that certain provisions of the industry standard will commence on 1 July 2025.

These include provisions relating to disconnections and reconnections (parts of section 13), prohibiting providers from requiring affected persons to engage with the perpetrator (subsection 15(1)), the obligation to publish information about available DFV support offered by the provider (section 16). These provisions support the immediate safety of affected persons and are capable of implementation without an extended lead time. Provisions relating to the development of a provider's DFV policy and DFV procedures (section 19) and the delivery of DFV training (sections 21 and 22) and the requirement to consult on the development of a provider's DFV policy, procedures and training (section 32) will also commence on 1 July 2025. To allow time for development and for consultation, the policy and procedures are not required to be in place until 6 months after 1 July 2025 for large providers and 9 months after 1 July 2025 for small providers. In relation to the training requirements in sections 21 and 22, the relevant training must be delivered by large providers within 9 months of 1 July 2025 and by small providers within 12 months of 1 July 2025.

Commencement of the other provisions of the Standard are delayed to allow for capacity-building requirements. These include obligations related to, monitoring and review of policies, procedures and personnel compliance (sections 23 and 24) and security, privacy and record-keeping (sections 25 – 31) These provisions commence:

- for large providers (those with 30,000 or more services in operation), on 1 January 2026 (see item 2 in column 1 of the table in section 2); and
- for small providers (those with fewer than 30,000 services in operation), on 1 April 2026 (for the application of these provisions to small providers, see subsection 4(2)).

This staggered approach supports a risk-based and proportionate implementation pathway, ensuring that consumers receive timely protections while recognising the varying capabilities and scale of providers across the telecommunications industry.

Section 3 Authority

This section identifies the provision of the *Telecommunications Act 1997* (the **Act**) that authorises the making of the instrument, namely subsection 125AA(1) of the Act.

Section 4 Application of industry standard

This section sets out the application of the Standard in accordance with subsection 125AA(1) of the Act.

Paragraph 4(1)(a) provides that the Standard applies to participants in the telecommunications industry as follows:

- subparagraph (i) applies the Standard to CSPs in their dealings with consumers; and
- subparagraph (ii) applies the Standard to carriers in relation to their supply of carriage services to CSPs.

Paragraph 4(1)(b) provides that the Standard is drafted to give effect to the objectives set out in section 7 of the Direction. These objectives include requiring telecommunications providers to take reasonable and appropriate steps to support the safety and privacy of consumers experiencing domestic, family or sexual violence.

Through the definition of "consumer", the Standard applies to CSPs that supply telecommunications products to residential, small business and NFP customers, recognising that services provided to or used by individuals in these groups may be associated with risk.

The inclusion of carriers within the scope of the Standard ensures that carriers are required to support the implementation of safety and privacy protections at a systems level. There is only one obligation placed on carriers under the Standard (see section 26). That is to provide reasonable assistance to a provider to enable compliance with the requirement to suppress calls to specified helpline numbers from appearing on bills or other records (see subsection 25(3)). As carriers play a foundational role in the delivery of telecommunications services and in the operation of billing, numbering and network infrastructure, their cooperation may be necessary to give practical effect to that consumer protection.

Section 5 Definitions

This section defines key terms used throughout the Standard.

Some other expressions used in the Standard are defined in the Act or in the *Acts Interpretation Act 1901*.

Section 6 References to other instruments

This section provides that in the Standard, unless the contrary intention appears:

- a reference to any other legislative instrument is a reference to that other legislative instrument as in force from time to time; and
- a reference to any other kind of instrument is a reference to that other instrument as in force or existing from time to time.

Part 2 – Sexual violence outside a domestic and family violence situation

Section 7 Requirement where a consumer has experienced sexual violence outside a domestic and family violence situation

Part 2 of the Standard is designed to provide consumers who disclose experiences of sexual violence outside a domestic and family violence context (defined as non-domestic sexual violence), with key support measures related to the supply of telecommunications products under the Standard. It requires a provider to treat such consumers as "affected persons" for the purposes of subsection 8(2), 10, 13, 14 and 15 which relate to information about available support, the provision of support, the collection of evidence, and access to support services.

Section 7 recognises that non-domestic sexual violence can give rise to similar safety, wellbeing, and telecommunications-related needs as domestic and family violence. Extending core telecommunications support to these consumers provides a consistent and trauma-informed response, without requiring distinctions between the types of violence that may be unclear or re-traumatising to disclose.

Part 3 - Providing support

Section 8 Requirement to advise affected persons of available support

Section 8 outlines a provider's obligations to make affected persons aware that there is support available to the affected person at the first opportunity when it is safe for the affected person to have that conversation. This requirement is designed to provide consumers experiencing domestic, family or non-domestic sexual violence with access to relevant assistance in a timely, safe, and informed manner.

Subsection 8(1) requires that, where a provider interacts with an affected person, for the purposes of subsection 8(2) (which covers the provision of information about available DFV support) and subsection 9(1) (which relates to the application of provisions relating to agreeing on a preferred communication method and discussion of support options) – the provider must confirm that it is safe for the affected person to communicate.

Under subsection 8(2) when the provider interacts with an affected person (and has confirmed it is safe to have the conversation as required by 8(1)), the provider must proactively inform the affected person about the availability of its DFV support. This includes:

- Paragraph 8(2)(a) – Advising that the provider can assist the affected person in accordance with the provider's DFV policy. This is intended to make affected persons aware that dedicated support is available to them.
- Paragraph 8(2)(b) – Informing affected persons if the provider has a specialised DFV team or trained personnel, and that the affected person may request to be put through to that team directly (known as a warm transfer). This helps to facilitate access to appropriately trained staff who can provide tailored and trauma-informed assistance.
- Paragraph 8(2)(c) – Advising the affected person that there are support organisations listed in the provider's DFV statement and where the statement can be accessed. This helps connect affected persons with external specialist services.

A provider is only required to provide this information when it has not been previously given.

Subsection 8(3) provides that, after delivering the required information under subsection (2), the provider must ask the affected person whether they wish to access further information or support. This reinforces a consumer-led approach and allows affected persons to engage with support at a pace and level that suits their individual needs.

Together, these provisions support a proactive and consistent approach to engagement with affected persons, and require all providers to offer timely and appropriate information to support consumer safety, choice, and access to help.

Section 9 Application of sections 10 and 11

This section provides that sections 10 and 11 of the Standard will apply when the affected person has indicated they want to receive more information under subsection 8(3) and the provider has received confirmation that it is safe for the affected person to communicate under subsection 8(1). Subsection

9(2) confirms that a provider does not need to comply with subsection 10(1) and 11(1) more than once. This is intended to help affected persons receive the information they want at the first opportunity it is safe for them to do so without placing an obligation on providers to provide such information during each interaction.

Section 10 Requirement to agree on a preferred communication method

Section 10 sets out the requirement for providers to establish a safe and appropriate method of communication with affected persons and those who have disclosed non-domestic sexual violence, and who have indicated they wish to receive further support from the provider.

Subsection 10(1) requires that, where an affected person has expressed interest in accessing further support, and the provider has received confirmation that it is safe to proceed with the conversation, the provider must advise the affected person of the communication methods offered by the provider and ask whether they have a preferred:

- method of communication (for example, phone, email, SMS); and
- time of day for receiving communications from the provider using that method.

This provision is designed to respect the affected person's safety, privacy and communication needs, so that the provider contact does not inadvertently place the person at increased risk.

Subsection 10(2) provides that the preferred communication method and time will constitute the "agreed communication method" for future interactions related to domestic and family violence. This agreement will remain in place unless and until the affected person requests a different communication method. This recognises that affected persons may need to revise their preferences over time as their personal circumstances change.

Subsection 10(3) requires that a provider must only use the agreed communication method when contacting an affected person about matters related to domestic and family violence. Exceptions to this requirement are limited to circumstances where:

- the provider is legally required to use a different communication method (e.g., under a court order or statutory obligation); or
- the affected person initiates contact through a different method and confirms that the provider can use that different communication method for the purposes of that interaction.

This section is fundamental to supporting victim-survivor safety and autonomy. The intention is that providers take proactive steps to minimise risks of inadvertent disclosure or contact that could lead to harm, while also promoting trust, flexibility and consistency in provider communications.

Section 11 Requirement to discuss support options

Section 11 sets out obligations for providers to have a structured and consumer-led conversation with affected persons who have indicated they want to access more information and support. It also requires providers to act on any instructions the person gives about safeguarding their telecommunications services.

Subsection 11(1) sets out the required steps a provider must take when they first interact with an affected person, where the person has requested support.

- Paragraph 11(1)(a) requires the provider to identify whether the affected person is the customer (i.e. account holder) or an end-user. This distinction is important because it determines what actions the provider can take and what information can be accessed or changed.

- Paragraphs 11(1)(b) and (c) – require the provider to explain:
    - where the affected person is the customer and there is as an authorised representative on the account, what that representative can access and inform the affected person that they can retain, change, or remove that representative; and
    - how affected persons can make changes to their account or update their information,

  Together these paragraphs support consumer control over account access and personal information and empower affected persons to take practical steps in managing their account and personal safety.
- Paragraph 11(1)(d) requires the provider to ask the affected person whether they have any concerns about their privacy, safety or security in relation to their telecommunications product or account.
- Paragraph 11(1)(e) provides that, where concerns are raised, the provider must explain the options available to help address those concerns, having regard to whether the person is a customer or end-user.
- Paragraph 11(1)(f) requires the provider to ask the affected person for their instructions about which of the discussed options they would like to adopt.

Subsection 11(2) provides that, where an affected person later informs the provider that their circumstances have changed and asks to update the instructions given under paragraph 11(1)(f), the provider must amend those instructions as requested. This allows for the support to remain responsive to the affected person's needs over time.

Subsection 11(3) confirms that providers must act in accordance with the instructions agreed with the affected person under section 11 as soon practicable. This reinforces that affected persons should be able to rely on the provider to implement their decisions about how best to manage their telecommunications products (being goods and services) as soon as practicable, in light of safety or privacy risks.

This section is intended to promote a trauma-informed and person-centred approach, by ensuring providers give affected persons a clear opportunity to raise concerns and adopt protective measures that meet their individual needs.

Section 12 Minimum requirements for support

Section 12 prescribes the minimum support options that providers must offer to affected persons under paragraph 11(1)(e), which requires providers to discuss options available to enhance the affected person's safety, privacy, and security.

Paragraph 12(a) requires that providers make available the option to set up a new telecommunications account that is not linked to the perpetrator. This is intended to assist affected persons to separate their telecommunications arrangements from those of a perpetrator and take steps to secure their account information.

Paragraph 12(b) requires providers to offer privacy, security and safety protections on the affected person's account. This may include requiring a PIN, password, or verification code sent to a safe number or email address nominated by the affected person or within a mobile application. These measures are designed to enhance protections that help prevent unauthorised access to accounts and communications and to safeguard sensitive personal information.

The minimum support requirements are intended to make a consistent baseline of safety-related assistance to all affected persons across all providers, while allowing for additional support to be offered where appropriate. Pursuant to subsection 9(2), these options do not have to be offered to in every discussion. However, when discussing privacy safety and security options with an affected person under paragraph 11(1)(e) these options must be offered.

Section 13 Providing support to affected persons

Section 13 sets out further obligations on providers once an affected person has sought assistance from a provider.

Subsection 13(1) requires providers to keep the affected person informed about the matter on which they have sought assistance. These communications must be via the agreed communication method, if one is in place. This is to keep the affected person informed and aware of the status of the assistance and support they have sought which may have direct impacts on their safety and security. It also means communication remains safe and appropriate to the person's circumstances.

Subsection 13(2) imposes obligations when an affected person expresses safety concerns:

- Paragraph 13(2)(a) requires the provider to prioritise assisting the person in relation to their telecommunications service; and
- Paragraph 13(2)(b) prohibits disconnection, restriction or suspension of the service for 30 days or a longer period as agreed between the provider and the affected person if the person is the customer of the account. Disconnection, restriction or suspension can occur where it is requested by the affected person.

Subsection 13(3) provides that where a telecommunications service has been restricted, suspended or disconnected and the affected person requests reversal of that action because of a domestic and family violence-related safety risk, the provider must reverse the action as a matter of urgency. The provision requires that the provider must reverse the action the first time that the affected person contacts the provider and raises the domestic and family violence-related safety risk.

Subsection 13(4) provides that if reversing the action under subsection 13(3) is not practical, the provider must offer an equivalent telecommunications service. The intention of this provision is so the affected person is not left without access to communications services essential to their safety and security. For example, if an affected person who is an end-user has their service disconnected by a customer it may not be possible for the provider to reconnect that specific service. However, this provision requires the provider to offer the affected person an equivalent service. Under this requirement if an affected person has a mobile phone service and an internet service that is used to support security cameras, the provider must offer equivalent services appropriate to the their needs.

Subsection 13(5) provides that reversal of a disconnection, restriction or suspension of a service is not required where the reversal would contravene another law of the Commonwealth.

Sections 65, 67 and 69 of the *Telecommunications (Emergency Call Service) Determination 2019* are an example of where the reversal would contravene another law of the Commonwealth as they prohibit the supply of carriage services to a mobile phone that is not configured to be able to access the emergency call service.

Subsection 13(6) requires that, where an affected person has sought assistance from the provider within the last 60 days, before initiating credit management action, providers must:

- take into account the potential impact on the affected person of such action at that time (13(6)(c)) and whether another person (such as the perpetrator) may be responsible for the

debt (13(6)(d)). This seeks to reduce the risk of re-traumatisation or financial harm to affected persons resulting from debt they did not incur or cannot safely address at that time.

- review the affected person's records to confirm that all agreed support actions – such as setting up payment plans or extensions – have been correctly implemented (13(6)(e)). This requirement seeks to prevent service interruptions that may inadvertently undermine the person's safety.

Taken together, these provisions are designed to provide affected persons with tailored, timely, and trauma-informed support from providers in remaining connected to telecommunications networks particularly in circumstances involving safety risks or financial vulnerability, while recognising legal and technical limitations.

Section 14 A provider must not require evidence

Section 14 limits the circumstances in which a provider may require an individual to provide evidence or supporting material to be recognised as an "affected person" for the purposes of the Standard. To minimise barriers to accessing support for affected persons it is expected that the collection of evidence should be a last resort.

Subsection 14(1) provides that providers must not require individuals to supply evidence to demonstrate that they are affected by domestic and family violence. This reflects best practice trauma-informed approaches and recognises that many affected persons may be unwilling or unable to provide documentary or other proof of abuse. Requiring such evidence can re-traumatise individuals or discourage them from seeking assistance.

Subsection 14(2) outlines two very limited exceptions to the general prohibition. Providers may request evidence:

- Paragraph 14(2)(a) - where the provider is under a legal obligation to do so (eg. subsection 11(3) of the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022* requires that a provider must keep a record of the basis on which the employee or agent of the provider reasonably believed that the requesting person was a person in vulnerable circumstances (which would include affected persons)); or

- Paragraph 14(2)(b) - where the provider reasonably requires it to protect the interests of an affected person. This could, for example, be used if the provider reasonably suspects a customer is claiming to be an affected person for the purpose of making changes to a service used by an affected person's account to interfere with their privacy, safety or otherwise perpetrate abuse.

Subsection 14(3) imposes safeguards on the use of these exceptions. Where a request for evidence is permitted, providers must:

- first consider whether existing internal records contain sufficient information to satisfy the requirement (e.g. the affected person has made a claim in relation to a telecommunications product or service, stating that it is not in their possession and they can show they are located in one State, and the call records of the provider show that the product or service is being used in a different State); and

- request only the minimum amount of evidence or information needed to satisfy the legal obligation or to protect the interests of the affected person.

The intent of section 14 is to minimise barriers for affected persons to access assistance under the Standard, while allowing for limited, justifiable exceptions grounded in legal compliance or risk mitigation related to DFV.

Section 15 Communications with an affected person

Section 15 imposes safeguards and standards so that providers communicate with affected persons in a respectful, safe, and trauma-informed manner.

Subsection 15(1) prohibits providers from requiring affected persons to contact or otherwise engage with their perpetrator or the perpetrator's authorised representative. This protects individuals from further trauma, intimidation, or safety risks that may arise from such interactions.

Subsection 15(2) provides that affected persons must not be required to disclose the details or nature of the abuse they have experienced in order to receive support. This recognises that affected persons should not be compelled to disclose this information to receive support from their provider and provides for an affected person to receive support that is accessible without barriers.

Subsections 15(3) and (4) establish requirements for warm transfers. Where an affected person is communicating with one staff member (the **transferor**) but needs to be transferred to another (the **transferee**) for appropriate support:

- Paragraph 15(3) requires the transferor to offer a warm transfer – which is defined in section 5 and means that the transferor must explain the details of the affected person's query to the transferee in the call or chat before transferring the query, to facilitate a continuous and supported handover.
- Subsection 15(4) requires the provider to carry out the warm transfer if the offer is accepted by the affected person.

These requirements are designed to prevent the affected persons being obligated to repeat information, which may be distressing. Personal information collected by a provider when actioning a "warm transfer" under section 15 should not be recorded to protect the privacy and security of affected persons (see subsection 31(3)).

Subsection 15(5) provides that, where an affected person raises domestic and family violence as a safety concern and makes a request about how their bill is to be received (e.g. requesting a change of delivery method or a billing address), the provider must comply with the request if it is able to do so. This supports safety planning and helps prevent inadvertent disclosure of the affected person's situation or location.

Together, the provisions in section 15 are designed to reduce the risk of further harm or re-traumatisation through provider communication practices, while also treating the affected persons with dignity, discretion, and care.

Part 4 –Requirements relating to availability of DFV support information

16 Requirement to publish, on commencement of this provision, information relating to available support for affected persons

Section 16 is an interim provision that applies from 1 July 2025 and requires providers to publish information that informs consumers about the provider's DFV-related supports and how to access relevant assistance that is available on commencement. This recognises the importance of consumers and affected persons having a clear and immediate understanding of what support is available to them and how to access that information.

Subsection 16(1) requires a provider to publish information on its website about what support it offers to affected persons and how the affected person can access that support. This information should refer to any DFV support the provider currently has in place at the commencement of the Standard.

Subsection 16(2) applies to providers who may not offer any specific support to affected persons at the commencement of the Standard. It requires that these providers publish specified information for affected persons. This includes:

- Paragraph (a) – information for one or more organisations that an affected person can contact for support in relation to domestic and family violence, including contact details, for example 1800RESEPECT or the details of a State or Territory DFV support service.
- Paragraph (b) – a statement that the provider will have DFV support in place by the date on which section 17 applies to them under the Standard (that is, 1 January 2026 for large providers and 1 April 2026 for small providers).
- Paragraph (c) – details of where the affected person should direct their queries for support from the provider until the provider's DFV support arrangements are in place.

This provision will cease operation on the day before the obligation to publish a DFV Statement under section 17 takes effect, which is 31 December 2025 for large providers, and on 31 March 2026 for small providers. This balances the need for appropriate consultation and implementation timeframes to deliver the requirements of section 17.

Section 17 Requirement to publish a DFV Statement

Section 17 requires providers to make publicly available a Domestic and Family Violence (DFV) Statement that informs consumers about the provider's DFV-related supports, commitments, and how to access relevant assistance.

Subsection 17(1) applies to all providers that offer telecommunications products to consumers. It requires those providers to publish a DFV Statement that includes information about how and where consumers can find DFV support.

Subsection 17(2) sets out the required content of the DFV Statement. This includes:

- A statement that the provider has procedures and policies in place to protect the safety of affected persons.
- A commitment to maintaining affected persons' telecommunications connectivity and, where services have been restricted, suspended or disconnected, to reversing those actions urgently if a safety concern is expressed or indicated. That statement must also confirm that a provider will – where reversal is not practical – offer an equivalent service.
- Recognition that domestic and family violence (and, non-domestic sexual violence) can be a reason for non-payment, and that affected persons may qualify for financial hardship support under the *Telecommunications (Financial Hardship) Industry Standard 2024*.
- Details on how consumers can contact the provider for DFV assistance, including contact methods, hours of operation, and how to request a call-back.
- Information about how to access support from one or more third-party DFV support organisations, (for example, 1800RESPECT).

Subsection 17(3) prescribes how the DFV Statement must be presented and made accessible. It must:

- be in written form, either print or digital;
- use clear, plain, and accurate language and be up to date;
- use a font style and size that is clear and easy to read;

- be accessible to consumers with disabilities, from culturally and linguistically diverse backgrounds, or with other support needs for example through offering the information in multiple languages and/or with access to interpreters;
- be clearly available on the provider's website homepage and, if applicable, through its mobile application;
- be made available during online chat interactions where a consumer self-identifies or is suspected to be an affected person and consents to receiving the statement.

These provisions promote transparency and facilitate consumer access to DFV-related support information, particularly for those in vulnerable circumstances.

Section 18 Requirements regarding access to DFV support services

Section 18 sets out minimum requirements for how providers must enable affected persons to contact them for DFV-related assistance. It supports timely and accessible communication, through channels that may be private from, or less accessible to, a perpetrator, to better meet the safety needs of affected persons.

Subsection 18(1) requires providers to offer at least two communication channels from a list of options. These may include a specialist DFV support phone line, a dedicated webform, online written chat, in-person assistance at a retail store, or an email address. Providers may offer more than the minimum number of channels if they choose.

Subsection 18(2) requires that at least one of the available communication channels under subsection (1) must connect the affected person to an individual member of the provider's personnel. This is intended to support access to trauma-informed and empathetic engagement, in order to build trust and deliver effective assistance.

Subsection 18(3) establishes that when an affected person requests the provider to initiate contact or to return a call, the provider must do so using either the agreed communication method or the method and time nominated by the affected person if that is supported by the provider. This provision prioritises safety and respects consumer preferences about how and when they can be contacted.

Subsection 18(4) mandates that personnel must be accessible during business hours to directly assist affected persons.

Collectively, these requirements contribute to a consistent and accessible approach to consumer engagement for people experiencing DFV across a range of communication platforms.

Part 5 – General requirements relating to policies and procedures

Section 19 Develop domestic and family violence policies and procedures

Section 19 establishes an obligation for CSPs to develop a DFV policy and DFV procedures that support effective compliance with the Standard and that are intended to promote consistent, safe, and informed interactions with affected persons.

Subsection 19(1) outlines the key components of this obligation.

- Paragraph (a) requires providers to establish a DFV policy that complies with the minimum content requirements in subsection 20(1). This policy should guide the provider's organisational response to DFV, including how it engages with affected persons and the principles that underpin its service delivery in this context.

- Paragraph (b) requires providers to develop DFV procedures that operationalise their DFV policy and ensure compliance with the broader requirements of the Standard. These procedures must meet the minimum requirements set out in subsection 20(2), and provide guidance to personnel on how to respond to DFV in practice. Subparagraphs (i)–(iii) make clear that these procedures must do more than reflect policy intent; they must enable frontline compliance and effective implementation of the Standard.

Subsection 19(2) requires that a provider must ensure that its DFV policy and DFV procedures are in place at all times after the end of 6 months from 1 July 2025, for large providers and after the end of 9 months for small providers.

Subsection 19(3) requires that providers must comply with both their DFV policy and DFV procedures. This reflects the intent that policies and procedures must be embedded into day-to-day operations and service practices, with staff trained and supported to act in accordance with them.

Subsection 19(4) places accountability for DFV governance at the highest level of the provider's organisation. It requires the most senior responsible executive, typically the Chief Executive Officer. to approve both the DFV policy and the DFV statement (a separate requirement under section 17), and to assume overall responsibility for the implementation and operation of the DFV procedures. The intention is that DFV responsiveness is integrated into organisational leadership, strategic oversight, and resource allocation.

This section is central to embedding systemic, whole-of-organisation approaches to DFV, in line with evidence that ad hoc, discretionary, or individual-led responses are insufficient to support affected persons safely and effectively. It does not prevent a CSP from including additional content in its DFV policy or procedures beyond the minimum requirements of the Standard.

Section 20 Minimum requirements for DFV policies and procedures

Section 20 sets out the minimum content requirements that must be addressed in a provider's DFV policy and DFV procedures. These minimum standards are intended to support consistency across the sector while allowing flexibility for providers to tailor their approach to their business model, services, and customer base.

Subsection 20(1) identifies eight matters that must be addressed in the DFV policy:

- Paragraph (a) requires the policy to be in writing, providing transparency and accountability.
- Paragraph (b) requires that the policy prioritise the safety of affected persons. This overarching principle must guide how services are delivered and how internal systems identify and manage risk and escalate and resolve concerns.
- Paragraphs (c) and (d) require the policy to set out how the provider will support and manage affected persons, and the options for assistance it can offer so that affected persons are provided with accessible and consistent information about what support is available, and how it may be tailored to their needs.
- Paragraph (e) requires the policy to address how the provider supports its personnel who engage with affected persons, recognising that this work can be complex, sensitive and emotionally taxing. Support may include training, supervision, or access to employee assistance programs.
- Paragraph (f) requires the provider to address how it will protect the privacy and security of affected persons, including through secure record-keeping and appropriate handling of personal information. This reflects a key concern raised by stakeholders about unauthorised disclosure or access by perpetrators.

- Paragraph (g) requires that the policy set out how inclusive design will be used in the development and review of the provider's systems, processes and telecommunications products, to identify and reduce risks to affected persons. This encourages providers to take a proactive, systems-based approach to DFV safety, rather than relying solely on reactive measures.
- Paragraph (h) requires the policy to address how the provider will use an intersectional approach in supporting affected persons (and, where applicable in accordance with section 7, those who have experienced non-domestic sexual violence). This type of approach to the policy recognises and responds to the diverse experiences and needs of affected persons, including those shaped by disability, race, cultural background, sexuality or gender identity and how this impacts their experiences of DFV and non-domestic sexual violence and accessing support. Consultation with appropriate experts in accordance with section 32 will support providers in this.

Subsection 20(2) specifies the required content for the provider's DFV procedures, which are intended to operationalise the policy and support safe, consistent engagement with affected persons. These procedural elements are key to frontline implementation and should be informed by good practice principles, including trauma-informed care.

- Paragraph (a) requires that procedures be trauma-informed. This means they must be designed to reduce the risk of re-traumatisation and to support interactions that are respectful, safe, and empowering for an affected person.
- Paragraph (b) requires procedures to set out how personnel can safely and appropriately identify, support and assist affected persons. This should include practical guidance on recognising signs of DFV, responding to disclosures, and managing complex account issues.
- Paragraph (c) requires providers to include guidance on how personnel can safely and appropriately engage with perpetrators where necessary – for example, when a perpetrator is an account holder or seeks access to services. Clear procedures in such cases are essential to managing risk and avoiding inadvertent harm.
- Paragraph (d) requires procedures to explain how staff will implement the requirements in subsections 27(1) and (2), which relate to collection, storage, privacy and security of personal information.
- Paragraph (e) requires that procedures include how personnel can manage and respond to DFV (and, where relevant, non-domestic sexual violence), including how and when to escalate matters internally. This ensures staff are supported in responding to risk and complexity.
- Paragraph (f) requires that actions agreed with affected persons – such as changes to account access – are recorded in ways that prevent inadvertent disclosure to perpetrators. This supports both safety and continuity of support.
- Paragraph (g) requires that procedures include steps to minimise the number of times an affected person is required to explain their circumstances, acknowledging the harm caused by repeated disclosure. This may involve consistent case management or internal information-sharing protocols that reduce the need for consumers to retell their story.

The obligations in Part 5 reflect both organisational accountability and the importance of safe, trauma-informed engagement with affected persons.

Part 6 Training

Section 21 Training for all personnel

This section establishes a requirement for telecommunications provider personnel (defined in section 5 as being those personnel who are involved (either directly or indirectly) with consumers in Australia) to receive training on the provider's DFV policy. The aim of this provision is to embed a basic level of DFV awareness and alignment across the organisation.

For clarity, it is not expected that roles with no association or influence over the outcomes for consumers in Australia receive training – for example, office cleaners, building maintenance staff, or other roles with no influence on outcomes for Australian consumers including personnel located overseas whose role has no impact on or association with Australian consumers.

The provision does require that DFV policy training is undertaken by all senior and upper management and staff who may not deal directly with consumers but whose work may play a role in services supporting affected consumers or who may encounter DFV issues indirectly in the course of their duties including areas like IT and HR.

Regarding the training for personnel located outside Australia, if the requirement or action which applies to the provider under the Standard is being implemented by those personnel, then those personnel must receive the relevant DFV training, irrespective of their location.

Subsection (1) requires providers to deliver this training, either directly or through a third-party individual or organisation with DFV expertise. This reflects the principle that training must be appropriately informed by contemporary understanding of DFV and consistent with good practice. Third-party involvement provides for training content that is expert-led, credible and grounded in lived experience and current research.

Subsection (2) sets out the timing for delivery of DFV policy training:

- Under paragraph (a), all existing personnel must be trained within nine months of the section's commencement for large providers and within 12 months of the section's commencement for small providers.
- New personnel must be trained within one month of their engagement.
- Under paragraph (b), personnel must complete refresher training on an annual basis so that awareness and capability is maintained over time.

Section 22 Training of customer facing personnel

This section builds on the organisation-wide obligation by setting additional requirements for specialised DFV training for customer-facing and other relevant personnel. The objective is that personnel most likely to interact with affected persons or encounter DFV-related issues are equipped with appropriate knowledge, skills and sensitivity to do so safely and effectively.

Subsection (1) identifies three key groups who must receive specialised DFV training:

- Paragraph (a) covers consumer-facing personnel who may be the first point of contact for affected persons, such as call centre or retail staff.
- Paragraph (b) extends coverage to personnel working in functional areas that are more likely to encounter DFV-related issues. These may include sales, financial hardship, credit management, fraud, privacy and complaint handling.

- Paragraph (c) relates to specialist DFV support personnel, where such roles exist. This may include personnel within teams or areas created to deal specifically with vulnerable consumers and/or with those affected by DFV or individual staff with specialist training in supporting individuals affected by DFV.

Subsection (2) outlines the required content for this training:

- Paragraph (a) requires that the training must cover the provider's DFV policy and DFV procedures, so that staff understand and can apply internal processes in practice.
- Paragraph (b) mandates training on the nature and impacts of DFV, with a specific focus on how DFV interacts with telecommunications services. This would include an understanding of the use of telecommunications in contributing to the safety and security of affected persons and as a potential tool for perpetrators in executing DFV.
- Paragraph (c) requires training to address how to identify affected persons. Identification may occur through disclosure or through recognition of indicators, consistent with good practice guidance. These may include irregular service patterns, restricted account access, unusual consumer behaviour, or third-party interference.
- Paragraph (d) addresses intersectionality, requiring training to build awareness of how multiple or compounding factors (such as race, age, geographic location, sexual orientation, ability, class, language, or economic dependence) may shape a consumer's experience of DFV and their support needs.
- Paragraph (e) requires training on how to engage with affected persons, including responding to affected persons where there is a change in their circumstances. It should focus on how to be responsive and adaptable to the person's needs in ways which reduce the risk of re-traumatisation.
- Paragraph (f) requires training to include how to recognise and safely engage with perpetrators while protecting the safety of affected persons and personnel. The intent is that staff are prepared and safe when a known or alleged perpetrator attempts to engage with the provider, for example by seeking account control or monitoring. The training should make clear that providers are not responsible for determining whether a person is a perpetrator. Rather, it is intended that the training must support staff to apply consistent, risk-aware responses – such as appropriate escalation, minimising risk of harm, and protecting staff safety.

Subsection (3) allows training to be tailored to suit the specific functions of relevant personnel. For example, a frontline sales agent may need different emphasis than a financial hardship specialist or a complaints manager, though core learning outcomes should be consistent.

Subsection (4) sets out the timing requirements for delivery of this specialised training:

- Under subparagraph (a)(i), personnel who deal directly with consumers when section 22 commences must be trained within nine months of the section's commencement for a large provider and within 12 months for a small provider.
- Subparagraph (a)(ii) provides that other relevant personnel must receive training before they commence consumer-facing roles.
- Paragraph (b) mandates annual refresher training, recognising that DFV risks and best practices evolve, and that ongoing capability development is essential.

The purpose of this section is that personnel in critical roles receive appropriate, expert-informed training to enable safe, consistent and supportive engagement with both affected persons and

perpetrators. This section promotes organisational readiness and consumer safety, consistent with a trauma-informed, person-centred approach.

Part 7 Monitoring and review

Part 7 establishes ongoing monitoring and review obligations so that providers' DFV policies and procedures remain effective and are embedded into day-to-day practice. The Part strengthens internal accountability, introduces a structured review cycle, and requires executive oversight. The framework is designed to support continuous improvement and timely remediation of compliance issues to safeguard affected persons.

Section 23 Requirement to review policy and procedures

This section requires that providers must monitor and review their DFV policy and DFV procedures at least every 24 months, so that these documents remain current, operationally relevant, and fit for purpose. This timeframe balances the need for periodic strategic review with the practical resource constraints of providers, particularly small providers.

In recognition of the dynamic nature of DFV risks and the importance of safety-centred responses, paragraph (b) requires earlier review if the provider becomes aware that its DFV policy or DFV procedures are not operating effectively to protect the safety of affected persons. This is intended to be a proactive requirement so that providers respond promptly to emerging risks or shortcomings, rather than waiting for the next scheduled review cycle.

This dual approach is designed to embed a continuous improvement mindset into DFV responses, aligning with principles from relevant regulatory and industry guidance, such as the Communications Alliance DFV Guideline, referred to above.

Section 24 Requirement to monitor personnel

Subsection (1) requires providers to develop and implement an internal monitoring program to assess personnel compliance with its DFV policy and DFV procedures. The intent is that the policy is not merely a formal requirement but is actively operationalised in frontline practice.

Subsection (2) imposes a clear remediation obligation where non-compliance by the provider's personnel is detected. Providers must act within 10 business days to address identified breaches. This promotes timely intervention while allowing time for investigation, internal decision-making, and corrective action.

Subsection (3) reinforces governance and accountability by requiring that the most senior responsible executive, as referenced at subsection 19(2), must approve the monitoring program. This is intended to ensure the provider's program has adequate senior-level visibility, resourcing, and accountability.

Subsection (4) mandates that the outcomes of the monitoring program be reviewed by the most senior responsible executive at least every six months, beginning six months after the section commences (for large providers) or applies (for small providers). This regular review cycle facilitates ongoing oversight and strategic responsiveness and encourages providers to take a data-driven approach to DFV compliance.

Subsection (5) requires a provider to make changes to its DFV policies and DFV procedures where the review of the monitoring program conducted in accordance with subsection (4) has identified it is not operating to protect the safety of affected persons. These changes must be made as soon as practicable, meaning that small procedural changes should be effected immediately while some more significant changes, which could require consultation with DFV experts, could reasonably be expected to take longer.

Together, sections 23 and 24 are designed to promote a robust internal assurance framework. These sections support the Standard's broader objectives of embedding DFV awareness and safe response capability across the telecommunications sector, with the intention that providers are actively maintaining and improving their capacity to support affected persons.

Part 8–Security and privacy

Part 8 sets out obligations for providers to safeguard the security and privacy of information relating to affected persons. These protections are critical to reducing the risk that telecommunications services are misused by perpetrators to monitor, control or harm consumers experiencing DFV.

Section 25 Requirements relating to the security and privacy of an affected person

Subsection (1) places clear limits on the disclosure and handling of information about affected persons. A provider must not disclose any information that could identify or locate an affected person, including their contact or financial details, without their consent, unless required by law.

Subsection (2) requires providers to provide a quick exit function on all of their webpages that relate to support for consumers experiencing DFV. This feature is intended to help affected persons leave a page (which they may not wish a perpetrator to see them viewing) quickly, and be directed to a safe page (such as the Google home page, or a daily weather site), if they are being monitored or feel unsafe.

To support privacy when accessing DFV services, subsection (3) requires providers to not record calls to support numbers, as specified in the definition of "support telephone numbers" in section 5 of the Standard, on any bills, call logs or other materials issued to a customer in relation to a service. This allows affected persons to seek support discreetly without fear of the interaction being visible to a perpetrator.

In addition, under subsection (4), providers may only access an affected person's personal information for a legitimate purpose directly related to management of the account, minimising the risk of inappropriate internal use.

Section 26 Requirement on carriers to provide assistance

Section 26 requires that carriers provide reasonable assistance so that a provider can meet the obligation in subsection 25(3), which prohibits recording calls to specified support telephone numbers on bills or other customer facing records. This obligation recognises that cooperation may be needed across wholesale and retail layers of service provision to implement technical solutions.

Section 27 Security of personal and sensitive information

Subsection (1) requires providers to securely store any information collected under the Standard about affected persons.

Subsection (2) requires providers to implement measures to protect that information from misuse, interference, loss, or unauthorised disclosure, particularly to a perpetrator.

Specific categories of sensitive information that must be protected include:

- details of arrangements made with the provider to support the affected person,
- the affected person's current address and billing details, and
- the fact that the person has been identified or self-identified as an affected person.

These requirements support a consistent baseline of information security practices across the sector.

Section 28 Privacy

Section 28 applies to providers who are not subject to the *Privacy Act 1988* (the **Privacy Act**), so that equivalent privacy protections apply when handling personal information they collect under the Standard.

Paragraph (a) requires that personal information is not used or disclosed except in the following circumstances:

- where information is disclosed to either the ACMA or TIO for the management of a complaint or investigations,
- with the express consent of the consumer, or
- as otherwise required or authorised under Australian law or a court or tribunal order.

Paragraph (b) requires providers to securely dispose of or destroy personal information once it is no longer required under the Standard or other applicable laws.

A note in the Standard clarifies that providers regulated under the Privacy Act remain subject to Australian Privacy Principle 6, which governs the use and disclosure of personal information.

This section aims to ensure consistency in privacy expectations across the industry.

Section 29 Where privacy is breached

Section 29 covers instances where there has been unauthorised access to or disclosure of personal information relating to an affected person. There are notification obligations under the *Privacy Act 1988,* about eligible data breaches which require providers to prepare a statement about the breach and as soon as practicable give a copy of the statement to the Information to the Commissioner and notify individuals whose personal information was involved in the breach (or publish the statement).

However, the immediate risk to the safety and security of an affected person whose personal information is involved is potentially higher as this could directly result in a perpetrator gaining access to sensitive information such as their current location. It is critical that affected persons can be assured that they will be informed within a set timeframe where such access or disclosure has occurred so they can take appropriate steps to manage any heightened risks to their safety.

Subsection (1) requires that where a provider becomes aware that an affected person's personal information has been accessed or disclosed without authorisation they must notify both the ACMA and the affected person within 2 days. This is separate to any obligations under the Privacy Act to notify the Office of the Australian Information Commissioner.

Subsection (2) covers situations where such notifications maybe inconsistent with the agreed communications method and allows for providers to wait until the notification can be made using the agreed communications method. This allows a provider to respect the safe communications method chosen by the affected person without contravening its obligation to notify them of the data breach.

Subsection (3) requires providers, when notifying the affected person, to provide contact details for a national or state-based DFV support service to assist with safety planning. This is to provide the affected persons with timely advice and support following a potential compromise of their information.

Taken together, these provisions provide affected persons with the information they need to react swiftly to mitigate potential risks to their safety and security.

Part 9—Record keeping

Part 9 sets out obligations for providers to maintain and manage records in a manner that supports compliance with the Standard, facilitates effective regulatory oversight, and upholds the privacy and safety of affected persons.

Section 30 Requirements to keep records

Subsection 30(1) requires providers to keep records sufficient to demonstrate compliance with the requirements of the Standard.

Subsection 30(2) places limits on the scope and handling of these records. Providers must:

- limit collection to information necessary to demonstrate compliance (paragraph (a)),
- take reasonable steps to protect information from misuse, interference, loss, and unauthorised access, modification or disclosure (subparagraph 30(2)(b)(i)), and
- ensure secure disposal or destruction of the information once it is no longer required under the Standard or other applicable laws (subparagraph 30(2)(b)(ii)).

These provisions support responsible data handling, consistent with broader privacy and data security principles. They also acknowledge the sensitive nature of information that may be collected in the context of family, domestic and sexual violence.

Section 31 Record retention

Section 31 sets minimum timeframes for retaining records and outlines circumstances where extended retention is required so that sufficient records are available to support complaint resolution and regulatory investigations. There is no expectation for the records to be retained beyond the period specified in this section.

Subsection 31(1) requires that providers:

- retain the records required under subsection 30(1) for at least two years, or for as long as the affected person continues to receive assistance under the Standard – whichever is longer (paragraph 31(1)(a)), and
- make the records available to the ACMA upon written request (paragraph 31(1)(b)).

Subsection 31(2) sets additional requirements where an affected person has made a complaint to a provider. In such cases, providers must retain relevant records:

- for a minimum of two years, or
- if the complaint is unresolved after two years, for a further 12 months after the date it is resolved.

Subsection 31(3) requires that, where practicable, records kept under subsection 31(1) must not include the personal information of an affected person. This reflects the importance of minimising risk to individuals who may be subject to serious safety concerns. Providers may balance minimising the retention of personal information with the obligation to have records demonstrating compliance by recording things such as where and what action has been taken, rather than specific personal details.

Subsections 31(4) and (5) establish specific safeguards for managing sensitive evidence obtained under subsection 14(2).

Where a provider requests and receives evidence to meet a legal obligation, the provider must only retain a copy or record for the duration necessary to meet the legal obligation (paragraph 31(4)(a)), and dispose of or destroy the material securely once the obligation has been met (paragraph 31(4)(b)).

Where evidence has been sought to prevent further harm to the affected person, the provider must dispose of or destroy the material securely once the evidence has been sighted (31(5)(a)).

In each case, the provider must retain a record of the type of evidence that was sought, provided and sighted (paragraph 31(4)(c) and 31(5)(b)).

This approach seeks to balance the need for providers to demonstrate compliance with protections that reduce the risk of misuse or unauthorised disclosure of sensitive personal information of affected persons.

Part 10—Consultation

This Part promotes the development of DFV policies, DFV procedures, and DFV training that are informed by lived experience, sectoral expertise and best practice.

Section 32 Requirement to consult

Section 32 requires providers to consult with relevant experts when developing and reviewing their DFV policies, procedures, and training, with the objective that provider responses to DFV are informed by specialist expertise, lived experience, and the needs of disproportionately affected groups.

Subsection 32(1) deals with to the development of DFV policies, procedures, and training while subsection 32(2) relates to when DFV policies and procedures are formally reviewed at least every 24 months.

Both subsection 32(1) and subsection 32(2) require providers to consult with at least two categories of stakeholders when developing or formally reviewing their DFV policy, DFV procedures, DFV policy training, and specialised DFV training. Specifically, providers must consult:

- a national or state-based DFV support service or organisation; and
- either:
    - a panel of individuals with lived experience of DFV, or their representatives; or
    - a national or state-based organisation representing communities who are or may be disproportionately affected by DFV – such as First Nations people, people with disability, culturally and linguistically diverse communities, and LGBTQIA+ individuals.

These requirements embed both sectoral expertise and diverse lived experience into the provider's DFV framework and reflect an intersectional approach to DFV responsive design. In consulting with DFV support service organisations, lived experience panels and those representing communities disproportionately affected by DFV, consultation may be undertaken through a single 'gateway' organisation who offers access to some or all these experts.

In respect to subsection 32(1), consultation may take place at any point during the development of the DFV policy, procedures and training. However, prior to conducting formal consultation, providers are encouraged to use existing DFV guidance and training materials – such as those developed by the telecommunications, energy, water or banking sectors – if those materials were developed in collaboration with the DFV support sector. This promotes efficient and consistent adoption of best practice resources while maintaining alignment with sector-informed approaches.

Subsections 32(3) and (4) differentiate consultation obligations based on provider size:

- Large providers (those with at least 30,000 services in operation) must undertake the required consultation directly.
- Small providers (those with 30,000 or fewer services in operation) may meet the consultation requirement through consultation conducted on their behalf by an industry group or representative body.

For clarity, under subsection (4) an industry group may consult with a DFV group on the development of a set of DFV policies and procedures which could then be customised by individual small providers for their own use.

This tiered approach recognises that smaller providers may have limited resources to engage stakeholders independently, while still providing for consultation that is meaningful and appropriately targeted.

Subsection 32(5) requires providers to consider the feedback obtained through consultation when developing and reviewing their DFV materials. It is expected that this feedback would be incorporated wherever practicable. This supports continuous improvement and responsiveness to stakeholder input, so that provider frameworks remain current, relevant and inclusive.

Part 11—Conferral of functions and powers

This Part clarifies the role of the **TIO** in relation to consumer complaints about compliance with this Standard.

Section 33 Conferral of functions and powers on the TIO

Under this section the TIO is granted specific powers in relation to complaints about matters covered by the Standard including:

- receiving, investigating and resolving consumer complaints;
- making determinations and issuing directions in relation to consumer complaints; and
- reporting on complaint trends.

This aligns with the TIO's existing remit to address consumer complaints about telecommunications services and supports accessible redress for affected persons.

Attachment B

Statement of compatibility with human rights

Prepared by the Australian Communications and Media Authority under subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011*

Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025

Subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* requires the rule-maker in relation to a legislative instrument to which section 42 (disallowance) of the *Legislation Act 2003* applies to cause a statement of compatibility with human rights to be prepared in respect of that legislative instrument.

The statement of compatibility set out below has been prepared to meet that requirement.

Overview of the Standard

The *Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025* (**the Standard**) has been made in accordance with the requirements set out in section 125AA of the *Telecommunications Act 1997* (**the Act**) and the *Telecommunications (Domestic, Family and Sexual Violence Consumer Protections Industry Standard) Direction 2024* (**the Direction**). It is drafted to meet the requirements and objectives in the Direction. In broad terms, those requirements and objectives are to ensure that carriers and carriage service providers (**providers**) in their dealings with telecommunications consumers take effective, timely and trauma-informed action to support those consumers who are, or may be, affected by domestic and family violence (**DFV**), and where relevant, sexual violence.

Human rights implications

The ACMA has assessed whether the instrument is compatible with human rights, being the rights and freedoms recognised or declared by the international instruments listed in subsection 3(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* as they apply to Australia.

Having considered the likely impact of the Standard and the nature of the applicable rights and freedoms, the ACMA has formed the view that the Standard engages the following rights or freedoms:

- The right to privacy in Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**), which states:

  1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

  2. Everyone has the right to the protection of the law against such interference or attacks.

- The right to freedom of expression in Article 19(2) of the ICCPR, which states:

  2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

- The right to protection against exploitation, violence and abuse contained in Article 20(2) of the ICCPR, and Article 6 of the Convention on the Elimination of All Forms of Discrimination against Women (**CEDAW**):
    - *Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law (Article 20(2) ICCPR)*
    - *States Parties shall take all appropriate measures, including legislation, to suppress all forms of traffic in women and exploitation of prostitution of women (Article 6 CEDAW)*

- The following rights for persons with disabilities under the Convention on the Rights of Persons with Disabilities (**the CRPD**):
    - *to access, on an equal basis with others, information and communications (Article 9); and*
    - *the right to freedom of expression and opinion, including the freedom to seek, receive and impart information and ideas on an equal basis with others and through all forms of communication of their choice (Article 21).*
- The right to equality and non-discrimination contained in article 20 of the ICCPR and article 3 of the CEDAW:
    - *1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. (Article 20 ICCPR)*
    - *States Parties shall take in all fields, in particular in the political, social, economic and cultural fields, all appropriate measures, including legislation, to ensure the full development and advancement of women, for the purpose of guaranteeing them the exercise and enjoyment of human rights and fundamental freedoms on a basis of equality with men (Article 3 CEDAW)*

Right to privacy

Article 17 of the ICCPR (like Article 16 of the Convention on the Rights of the Child and Article 22 of the CRPD) protects the right to freedom from unlawful or arbitrary interference with privacy. Certain provisions in the Standard could be considered to limit the right to privacy. However, the right to privacy is not an absolute right and a limitation may not be incompatible with the right itself.

Part 9 of the Standard imposes certain record keeping requirements on providers relating to their compliance with the requirements of the Standard. These records may include the personal information of consumers, and are required to be kept for at least 2 years, and be made available to the ACMA upon request.

The requirement for retention for at least 2 years is consistent with the requirement for retention of records applied in other record-keeping rules made by the ACMA under subsection 529(1) of the Act and reflects the reasonable and practical needs of the ACMA in performing its functions of monitoring and assessing compliance of providers with their obligations under the Standard. The ACMA's compliance and enforcement functions in relation to the Standard are integral to ensuring that providers are compliant with their obligations and that the objectives of the Standard and the Direction are met.

In the ACMA's view, the personal information required to be collected and kept by providers under the Standard is limited to that information which is necessary to enable the ACMA to investigate a complaint that a provider has breached the Standard.

Subsection 31(3) of the Standard provides that, where practicable, records kept under the Standard must not contain the personal information of an affected person.

Subsection 14(1) of the Standard requires that a provider must not require evidence or supporting material which demonstrates that a consumer is an affected person. The exceptions to subsection 14(1) are in subsection 14(2) which permit the collection of evidence that a consumer is an affected person (which may include personal information) in limited circumstances and if it is strictly necessary to comply with a legal obligation or it is necessary to protect the interests of a person affected by DFV.

Under subsections 31(4) and 31(5), records of information collected under subsection 14(2) must be destroyed or disposed of in a secure manner after those records have been sighted or are no longer needed to fulfil the legal obligation.

The Privacy Act 1988 (**the Privacy Act**) applies to the ACMA and the ACMA's administration of the Standard. As noted above, customer records may need to be accessed for monitoring and enforcement activities. The ACMA is subject in all relevant respects to the Privacy Act and the Australian Privacy Principles, and has a formal Privacy Management Plan, and takes all the usual precautions and other measures which a Commonwealth Government agency is required to take in order to safeguard personal information that comes into its custody and care.

Most providers are also subject to the Privacy Act regarding the personal information they handle in accordance with the Standard. In any event, it is expected that any personal information collected under the Standard would usually be provided with the consent of the consumer.

The Standard includes provisions in Part 8 which require providers to ensure that the information kept under that Part is only disclosed in specified circumstances, protected, stored securely and disposed of when no longer needed under the Standard or any other applicable laws. Further, section 28 of the Standard imposes requirements on providers that are not covered by the Privacy Act, to ensure that relevant personal information is kept confidential and not disclosed to third parties except: as required to manage a complaint made to the TIO or the ACMA; with the express consent of the consumer; or where disclosure is otherwise required or authorised by law.

Additionally, there is an obligation in section 29 for providers to inform the ACMA and the affected person of unauthorised disclosure.

These safeguards, together with the other restrictions on the handling of personal information mentioned above, indicate that the Standard is reasonable, necessary and proportionate.

Right to freedom of expression

The ACMA considers that the Standard engages the right to freedom of expression, in so far as that right includes the right of customers to receive information relating to domestic and family violence assistance in relation to their telecommunications products, as well as information about third party DFV support organisations.

Parts 3 to 5 of the Standard impose requirements on providers to provide information and advice to affected persons. For example: Part 3 requires providers to advise affected persons about available support and how the provider can assist them and communicate with them. Part 4 requires providers to publish information about how affected persons can access specific DFV support from the provider and other DFV support services, and to provide several communication methods for affected persons

to directly access DFV support services. Part 5 requires providers to establish a domestic and family violence policy and procedures with a number of minimum content requirements.

The obligations in Parts 3 to 5 of the Standard are designed to ensure providers have policies and procedures to assist customers affected by domestic and family violence, and to assist them to make informed decisions about how they can contact their provider for assistance and the options for assistance that a provider offers. As such, the standard affords protections to affected persons and is directed at promoting the rights of consumers to receive information about and options for DFV assistance. Accordingly, the ACMA considers that the Standard does not cause any limitation or interference with the right to freedom of expression.

Right to protection against exploitation, abuse and violence

The Standard promotes this right as it imposes obligations on providers to develop and implement policies and procedures to safely assist individuals who are victims of domestic or sexual violence to stay connected to their telecommunications service. The Standard imposes requirements on providers to prioritise affected persons' safety. Part 3 imposes obligations on providers to not require evidence that an individual is an affected person, and to identify and respond to affected persons' safety concerns in relation to their telecommunications products and accounts, such as by setting up new accounts not linked to a perpetrator and to discuss communication methods with affected persons. Part 5 includes obligations on how a provider's personnel can record information in a way that prevents disclosure to perpetrators of DFV. Part 6 also imposes obligations on providers to train personnel to be able to identify affected persons and to support affected persons effectively. Part 8 imposes obligations on providers to store information about affected persons in a way that prevents disclosure to perpetrators.

Rights for persons with disabilities

A number of provisions in the Standard positively engage and support the rights of people with disabilities (among others) to receive information on an equal basis, to choose a preferred form of communication about telecommunication products and to access DFV support consistent with Articles 9 and 21 of the CRPD.

For example, section 18 imposes obligations on providers to make a DFV statement which outlines their DFV policies and procedures, available in a format that is accessible to consumers with disabilities (among others). Further, section 32 requires providers to consult with national or state-based organisations that represent (among others) individuals with disabilities.

Right to equality and non-discrimination

The standard promotes this right by imposing obligations on providers to develop and review their DFV policies, procedures and training in consultation with various groups who may be disproportionately affected by DFV in different ways. Part 10 imposes obligations to consult with individuals with disabilities, First Nations peoples, individuals from culturally and linguistically diverse backgrounds and members of the LGBTQIA+ community.

Conclusion

The Standard is compatible with human rights because, to the extent that the right to privacy is limited by the Standard, in light of the clear protections and safeguards set out in the Standard, the limitation is reasonable, necessary and proportionate to meet the objectives of the Standard, and is no more restrictive than is required to achieve those objectives.

Further, the Standard is compatible with the right to freedom of expression, the right to protection against exploitation, abuse and violence, rights for persons with disabilities and rights to equality and

non-discrimination. These rights are positively engaged by providing consumer protections and safeguards by requiring providers to make information available about their DFV policies and procedures to all consumers on an equal basis, and by requiring them to prioritise the safety of consumers who have indicated that they are affected by DFV when supporting and communicating with such consumers. A range of safeguards set out in the Standard (as described above) bolster the Standard's compatibility with the various human rights is engages.