Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024

I, Julie Inman Grant, eSafety Commissioner, determine the following industry standard.

Dated

DRAFT ONLY—NOT FOR SIGNATURE

Julie Inman Grant
eSafety Commissioner

Contents

Part 1—Preliminary

1 Name

This is the *Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024*.

2 Commencement

This industry standard commences on the day that is 6 months after the later of:

(a) the day after the day on which it is registered under the Act; and

(b) the day after the day on which it is registered under the *Legislation Act 2003*.

3 Authority

This industry standard is determined under section 145 of the *Online Safety Act 2021*.

4 Object of this industry standard

The object of this industry standard is to improve online safety for Australians in respect of class 1A material and class 1B material, including by ensuring that providers of relevant electronic services establish and implement systems, processes and technologies to manage effectively risks that Australians will solicit, generate, distribute, get access to or be exposed to class 1A material or class 1B material through the services.

5 Application of this industry standard

(1) This industry standard applies to a relevant electronic service, wherever it is provided from, but only so far as it is provided to end-users in Australia.

(2) If:

(a) this industry standard applies to a relevant electronic service; and

(b) another industry standard, or an industry code, applies to the service; and

(c) the service's predominant functionality is more closely aligned with the other industry standard or the industry code;

this industry standard does not apply to the service.

Part 2—Interpretation

Note: A number of expressions used in this industry standard are defined in the Act, including the following:

(a) child;
(b) class 1 material;
(c) class 2 material;
(d) Classification Board;
(e) Commissioner;
(f) computer game;
(g) consent;
(h) electronic service;
(i) material;
(j) parent;
(k) posted;
(l) publication;
(m) relevant electronic service;
(o) removed;
(o) service.

6 General definitions

Definitions

(1) In this industry standard:

acceptable use policy, for a relevant electronic service, means the provisions of the terms of use for the service that regulate the use of the service by end-users.

account holder, for a relevant electronic service, means the person who is the counterparty to an agreement with the provider of the service for the provision of the service.

Example: A relevant electronic service may be provided to a family, where a parent or carer has the agreement with the provider of the service. The parent or carer is the account holder. Family members (including the parent or carer who is the account holder) who use the service are end-users.

Act means the *Online Safety Act 2021*.

appropriate action: see section 12.

Australian child means a child who is in Australia.

child sexual abuse material means material that:

(a) describes, depicts, promotes or provides instruction in child sexual abuse; or
(b) is known child sexual abuse material.

child sexual exploitation material means material that:

(a) is or includes material that promotes, or provides instruction in, paedophile activity; or
(b) is or includes:

(i) child sexual abuse material; or

(ii) exploitative or offensive descriptions or depictions involving a person who is, appears to be or is described as a child; or

(c) describes or depicts, in a way that is likely to cause offence to a reasonable adult, a person who is, appears to be or is described as a child (whether or not the person is engaged in sexual activity);

and, in the case of a publication, also includes material that is or includes gratuitous, exploitative or offensive descriptions or depictions of:

(d) sexualised nudity; or

(e) sexual activity involving a person who is, appears to be or is described as a child.

class 1A material means class 1 material so far as it comprises:

(a) child sexual exploitation material; or

(b) pro-terror material; or

(c) extreme crime and violence material.

Note: For the definition of ***class 1 material*** see section 106 of the Act.

class 1B material means class 1 material so far as it comprises:

(a) crime and violence material (but not extreme crime and violence material); or

(b) drug-related material.

Note: For the definition of ***class 1 material*** see section 106 of the Act.

classified means classified under the *Classification (Publications, Films and Computer Games) Act 1995*.

Note: RC is a classification.

closed communication relevant electronic service means a relevant electronic service the primary functionality of which is to enable an end-user in Australia:

(a) to create a list of other end-users of the service (***target end-users***); and

(b) to access and communicate with target end-users on that list;

where the first end-user has the target end-users' contact details otherwise than from the service, but does not include a service that is able to recommend target end-users to end-users in Australia based on interests or connections common to the end-users.

compliance report means a report required by section 37 or under subsection 38(2).

crime and violence material, in relation to a computer game, means material that is a computer game and that, without justification:

(a) promotes, incites or instructs in matters of crime or violence, or is or includes detailed instruction in, or promotion of, matters of crime or violence; or

(b) is or includes depictions of bestiality or similar practices; or

(c) depicts, expresses or otherwise deals with matters of crime, cruelty or violence in such a way that it offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that it should be classified RC; or

(d) is or includes depictions of violence that:

(i) have a very high degree of impact; and

(ii) are excessively frequent, prolonged, detailed or repetitive; or

(e) is or includes depictions of cruelty or realistic violence that:

(i) have a very high degree of impact; and

(ii) are very detailed; or

(f) is or includes depictions of actual sexual violence; or

(g) is or includes depictions of implied sexual violence related to incentives or rewards.

crime and violence material, in relation to a publication, means material that is, or is included in, the publication and that, without justification:

(a) promotes, incites or instructs in matters of crime or violence, or is or includes detailed instruction in matters of crime or violence; or

(b) is or includes realistic depictions of bestiality; or

(c) depicts, expresses or otherwise deals with matters of crime, cruelty or violence in such a way that it offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that it should be classified RC; or

(d) is or includes gratuitous, exploitative or offensive descriptions or depictions of violence that:

(i) have a very high degree of impact; and

(ii) are excessively frequent, emphasised or detailed; or

(e) is or includes gratuitous, exploitative or offensive descriptions or depictions of cruelty or real violence that:

(i) have a very high degree of impact; and

(ii) are very detailed; or

(f) is or includes gratuitous, exploitative or offensive descriptions or depictions of sexual violence.

crime and violence material, in relation to material that is not a computer game or a publication, means material that, without justification:

(a) promotes, incites or instructs in matters of crime or violence, or is or includes detailed instruction in matters of crime or violence; or

(b) is or includes depictions of bestiality or similar practices; or

(c) depicts, expresses or otherwise deals with matters of crime, cruelty or violence in such a way that it offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that it should be classified RC; or

(d) is or includes gratuitous, exploitative or offensive depictions of violence that:

(i) have a very high degree of impact; or

(ii) are excessively frequent, prolonged or detailed; or

(e) is or includes gratuitous, exploitative or offensive depictions of cruelty or real violence that:

(i) have a very high degree of impact; and

(ii) are very detailed; or

(f) is or includes gratuitous, exploitative or offensive depictions of sexual violence.

dating service means a relevant electronic service the primary functionality of which is:

(a) to solicit, offer, promote or provide access to dating, relationship, compatibility, matrimonial, social or romantic referral services; and

(b) to enable end-users to communicate with other end-users online;

but does not include such a service to the extent that its functionality is to connect end-users who offer their services for payment.

Note: Examples of services for payment are escort or prostitute services.

development program means a program required by section 23.

drug means a chemical, compound, or other substance or thing, that is included in Schedule 4 of the *Customs (Prohibited Imports) Regulations 1956*.

drug-related material, in relation to a computer game, means material that, without justification:

(a) depicts the unlawful use of drugs in connection with incentives or rewards; or

(b) depicts interactive, detailed and realistic use of drugs, being unlawful use; or

(c) depicts, expresses or otherwise deals with matters of drug misuse or addiction in such a way that the material offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should be classified RC; or

(b) is or includes detailed instruction in the unlawful use of drugs.

drug-related material, in relation to a publication, means material that, without justification:

(a) depicts, expresses or otherwise deals with matters of drug misuse or addiction in such a way that the material offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should be classified RC; or

(b) is or includes detailed instruction in the unlawful use of drugs.

drug-related material, in relation to material that is not a computer game or a publication, means material that, without justification:

(a) depicts, expresses or otherwise deals with matters of drug misuse or addiction in such a way that the material offends against the standards of

morality, decency and propriety generally accepted by reasonable adults to the extent that the material should be classified RC; or

(b) is or includes detailed instruction in the unlawful use of drugs; or

(c) is or includes material promoting the unlawful use of drugs.

end-user, of a relevant online service, means a natural person who uses the service.

Example: A relevant electronic service may be provided to a family, where a parent or carer has the agreement with the provider of the service. The parent or carer is the account holder. Family members (including the parent or carer who is the account holder) who use the service are end-users.

enforcement authority means:

(a) a police force or other law enforcement authority; or

(b) an organisation (including a non-government organisation) the functions of which include receiving reports of child sexual exploitation material or pro-terror material and facilitating making those reports to law enforcement authorities.

enterprise relevant electronic service means a relevant electronic service:

(a) the account holder for which is an organisation (and not an individual); and

(b) the primary functionality of which is to enable the account holder, in accordance with the terms of use for the service, to make the service available to a specified class of persons to facilitate communications between those persons; and

(b) that is of a kind that is usually acquired by account holders for the purpose mentioned in paragraph (b).

exploitative, in relation to a description or depiction of an event, means that the description or depiction:

(a) appears intended to debase or abuse, for the enjoyment of readers or viewers, the person or entity described or depicted; and

(b) has no moral, artistic or other value.

extreme crime and violence material, in relation to a computer game, means material that is crime and violence material in relation to a computer game where, without justification, the impact of the material is extreme because:

(a) the material is more detailed; or

(b) the material is realistic rather than stylised; or

(c) the game is highly interactive; or

(d) the gameplay links incentives or rewards to high impact elements of the game; or

(e) for any other reason.

extreme crime and violence material, in relation to a publication, means material that is crime and violence material in relation to a publication where, without justification, the impact of the material is extreme because of the emphasis, tone,

frequency, context and detail of the relevant elements of the publication and other factors that heighten impact.

extreme crime and violence material, in relation to material that is not a computer game or a publication, means crime and violence material where, without justification, the impact of the material is extreme because:

(a) the material is more detailed; or

(b) the material is highly interactive; or

(c) the relevant depictions in the material are realistic, prolonged or repeated; or

(d) for any other reason.

gaming service with communications functionality means a relevant electronic service the primary functionality of which is:

(a) to enable end-users in Australia to play online games with other end-users; and

(b) to enable sharing of user-generated URLs, hyper-linked text, images or videos between end-users;

but does not include

(c) a closed communication relevant electronic service; or

(d) a gaming service with limited communications functionality; or

(e) a service that limits the sharing of user-generated material between end-users to any or all of the following:

(i) in-game images or footage;

(ii) user-generated designs (such as environments and artwork);

(iii) virtual objects or maps;

(iv) pre-selected messages;

(v) non-hyper-linked text that is subject to automated filtering technology; or

(vi) ephemeral voice interactions.

gaming service with limited communications functionality means a relevant electronic service, other than a closed communication relevant electronic service, the primary functionality of which is to enable end-users in Australia to play online games with other end-users without enabling the sharing of user-generated URLs, hyper-linked text, images or videos between end-users (other than material of a kind referred to in paragraph (e) of the definition of gaming service with communications functionality in this subsection).

industry code has the meaning given in section 132 of the Act.

justification: see subsection (2).

known child sexual abuse material means material that:

(a) is or includes images (either still images or video images); and

(b) has been verified as child sexual abuse material by a governmental (including multi-lateral) or non-governmental organisation:

(i) the functions of which are or include combating child sexual abuse or child sexual exploitation; and

(ii) in the case of a non-governmental organisation—that is generally recognised as expert or authoritative in that context; and

(c) is recorded on a database that:

(i) is managed by an organisation of a kind described in paragraph (b); and

(ii) is made available to government agencies, enforcement authorities and providers of relevant electronic services for the purpose of their using technological means to detect or manage child sexual abuse material on relevant electronic services.

Example: An example of a database referred to in paragraph (c) is the database managed by the National Center for Missing & Exploited Children.

known pro-terror material means material that has been verified as pro-terror material.

Note 1: ***Known pro-terror material*** may include material that can be detected via hashes, text signals, searches of key words terms, or URLs or behavioural signals or patterns, that signal or are associated with online materials produced by terrorist entities that are on the United Nations Security Council's Consolidated List.

That List was accessible, on the registration of this industry standard, at https://www.un.org/securitycouncil/content/un-sc-consolidated-list.

Note 2: Material may, for example, be verified as a result of a decision of the Classification Board. Material may also be verified by using tools provided by independent organisations that are recognised as having expertise in counter-terrorism. Examples of these organisations include Tech against Terrorism and the Global Internet Forum to Counter Terrorism.

offensive: see subsection (3).

open communication relevant electronic service means a relevant electronic service the primary functionality of which is:

(a) to enable end-users in Australia to view, search for or communicate with other end-users (***target end-users***) on the service without knowing the target end-users' contact details; or

(b) to recommend target end-users to end-users in Australia, based on interests or connections common to the end-users.

To avoid doubt, it includes a relevant electronic service that enables an end-user to invite, through use of an internet link, another end-user to communicate with the first end-user.

pre-assessed relevant electronic service means each of the following:

(a) a closed communication relevant electronic service;

(b) a dating service;

(c) a gaming service with communications functionality;

(d) an open communication relevant electronic service.

pro-terror material means:

(a) material that:

(i) directly or indirectly counsels, promotes, encourages or urges the doing of a terrorist act; or

(ii) directly or indirectly provides instruction in the doing of a terrorist act; or

(iii) directly praises the doing of a terrorist act in circumstances where there is a substantial risk that the praise might have the effect of a leading a person (regardless of the person's age or any mental impairment that the person might suffer) to engage in a terrorist act; or

(b) material that is known pro-terror material.

However, material accessible using a relevant electronic service is not pro-terror material if its availability on the service can reasonably be taken to be part of public discussion, public debate, entertainment or satire.

provide a relevant electronic service includes make the service available.

provider, in relation to a telephony relevant electronic service, has the meaning given to ***carriage service provider*** in section 87 of the *Telecommunications Act 1997*.

RC means the "Refused Classification" classification under the National Classification Code.

risk assessment means an assessment of a kind required by subsection 8(1).

risk profile, for a relevant electronic service, means the risk profile of the service worked out under subsection 8(7).

sexual activity is not limited to sexual intercourse.

store: material is ***stored on a relevant electronic service*** if it is:

(a) in storage used for the service; or

(b) accessible through or using the service.

telephony relevant electronic service means a short messaging service (SMS) or a multimedia messaging service (MMS) provided over a public mobile telecommunications service as defined in in subsection 32(1) of the *Telecommunications Act 1997*.

terrorist act has the meaning given by section 100.1(1) of the *Criminal Code* (no matter where the action occurs, the threat of action is made or the action, if carried out, would occur).

terms of use, for a relevant electronic service, means the provisions of the agreement under which the service is provided and includes anything that may reasonably be regarded as the equivalent of terms of use.

Tier 1 relevant electronic service means a relevant electronic service:

(a) that is a Tier 1 relevant electronic service under paragraph 8(7)(a); or

(b) that is determined under subsection 8(9) to be a Tier 1 relevant electronic service.

Tier 2 relevant electronic service means a relevant electronic service that is a Tier 2 relevant electronic service under paragraph 8(7)(b).

violence means an act of violence or an obvious threat of an act of violence.

young Australian child means Australian child who is under 16.

Justification

(2) For this industry standard, in determining whether material is without justification, the matters to be taken into account include:

(a) the standards of morality, decency and propriety generally accepted by reasonable adults; and

(b) the literary, artistic or educational merit (if any) of the material; and

(c) the general character of the material, including whether it is of a medical, legal or scientific character; and

(d) the persons or class of persons to or amongst whom it is published or is intended or likely to be published.

Offensive material

(3) The question whether material is offensive for the purposes of this industry standard is to be determined in accordance with the Act, including section 8 of the Act.

7 Technical feasibility

In considering whether it is or is not technically feasible for the provider of a relevant electronic service to take a particular action, the matters to be taken into account include:

(a) the expected financial cost to the provider of taking the action; and

(b) whether it is reasonable to expect the provider to incur that cost, having regard to the level of the risk to the online safety of end-users in Australia of not taking the action.

Part 3—Risk assessments and risk profiles

8 Requirement to carry out risk assessments and determine risk profiles of relevant electronic services

Risk assessments to be carried out

(1) The provider of a relevant electronic service must, at the times required by and in accordance with this Part, carry out an assessment of the risk that class 1A material or class 1B material:

(a) will be generated or accessed by, or distributed by or to, end-users in Australia using the service; and

(b) will be stored on the service.

Note: See also paragraph 33(b).

Timing of risk assessments

(2) If the provider of the service was providing the service before the commencement of this industry standard, the risk assessment must be carried out as soon as practicable after, but no later than 6 months after, the commencement of this industry standard.

(3) Subsection (2) does not apply if a risk assessment that met the requirements of this Part had been carried out in respect of the service within 6 months before the commencement of this industry standard.

(4) A person must not start to provide a relevant electronic service to an end-user in Australia unless a risk assessment of the service has been carried out in accordance with this Part within 6 months before the person started to provide the service.

(5) The provider of a relevant electronic service must not make a material change to the service unless:

(a) a risk assessment of the service, as proposed to be changed, has been carried out in accordance with this Part; or

(b) the change will not increase the risk of class 1A material or class 1B material being accessed by, or distributed to, end-users in Australia using the service, or being stored on the service.

Certain services exempt from risk assessment requirements

(6) Subsections (1) and (4) do not apply to any of the following:

(a) an enterprise relevant electronic service;

(b) a gaming service with limited communications functionality;

(c) a pre-assessed relevant electronic service;

(d) a relevant electronic service that is determined under subsection (9) to be a Tier 1 relevant electronic service.

Note: However, subsection (1) applies to a relevant electronic service mentioned in this subsection if the service is materially changed.

Risk profiles of relevant electronic services

(7) The risk profile of a relevant electronic service is worked out as follows:

(a) if the risk that class 1A material or class 1B material will be solicited or accessed by, or distributed to, end-users in Australia using the service, or will be stored on the service, is high—the service is a Tier 1 service;

(b) if the risk that class 1A material or class 1B material will be solicited or accessed by, or distributed to, end-users in Australia using the service, or will be stored on the service, is medium—the service is a Tier 2 service.

(c) if the risk that class 1A material or class 1B material will be solicited or accessed by, or distributed to, end-users in Australia using the service, or will be stored on the service, is low—the service is a Tier 3 service.

(8) The provider of a relevant electronic service that conducts a risk assessment of the service must, on completion of the assessment, determine, in accordance with subsection (7), what the risk profile of the service is.

(9) However, the provider of a relevant electronic service may, at any time, without having conducted a risk assessment, determine that the risk profile of the service is Tier 1.

Note: See also paragraph 33(1)(b).

9 Methodology, risk factors and indicators to be used for risk assessments and risk profile determinations

Requirement for plan and methodology

(1) If the provider is required by this Part to carry out a risk assessment for a service, the provider must formulate in writing a plan, and a methodology, for carrying out the assessment that ensure that the risks mentioned in subsection 8(1) in relation to the service are accurately assessed.

(2) The provider must ensure that the risk assessment is carried out in accordance with the plan and methodology.

(3) The provider must ensure that a risk assessment is carried out by persons with the relevant skills, experience and expertise.

Forward-looking analyses of likely changes

(4) As part of a risk assessment carried out as required by this Part, the provider must undertake a forward-looking analysis of:

(a) likely changes to the internal and external environment in which the service operates or will operate, including likely changes in the functionality of, or the scale of, the service; and

(b) the impact of those changes on the ability of the service to meet the object of this industry standard.

Note: For the object of this industry standard see section 4.

Matters to be taken into account

(5) Without limiting subsection (1), the methodology for the conduct of a risk assessment must specify the principal matters to be taken into account in assessing relevant risks, which must include the following, so far as they are relevant to the service:

(a) the predominant functionality of the service;

(b) the extent to which material posted on or distributed using the service will be available to end-users of the service in Australia;

(c) the terms of use for the service;

(d) the terms of arrangements under which the provider acquires content to be made available on the service;

(e) the ages of end-users and likely end-users of the service;

(f) the outcomes of the analysis conducted as required by subsection (4);

(g) safety by design guidance and tools published or made available by a government agency or a foreign or international body;

(h) the risk to the online safety of end-users in Australia in relation to synthetic material generated by artificial intelligence.

Note 1: Arrangements referred to in paragraph (d) may include provisions that, if complied with, will reduce the risk that class 1A material and class 1B material will be made available through the service.

Note 2: Examples of agencies mentioned in paragraph (g) are the Commissioner or the Digital Trust & Safety Partnership Safe Framework.

10 Documenting risk assessments and risk profiles

(1) As soon as practicable after determining the risk profile of a relevant electronic service, the provider of the service must record in writing:

(a) details of the determination; and

(b) details of the conduct of any related risk assessment;

sufficient to demonstrate that the determination and the risk assessment were made or carried out in accordance with this Part.

(2) The record must include the reasons for the results of the assessment and the determination of the risk profile.

Note: See also paragraph 33(b).

Part 4—Online safety compliance measures

Division 1—Preliminary

11 This Part not exhaustive

This Part does not prevent the provider of a relevant electronic service from taking measures, in addition to and not inconsistent with those required by this Part, to improve and promote online safety for Australians.

12 What is appropriate action?

In determining whether action taken or proposed in relation to a relevant electronic service as required by this industry standard is appropriate, the matters to be taken into account include:

(a) the extent to which the action achieves the object of this industry standard in relation to the service; and

(b) if the action relates to a breach of applicable terms of use of a relevant electronic service, or community standards, in relation to class 1A material or class 1B material:

(i) the nature of the material and the extent to which the breach is inconsistent with online safety for end-users in Australia; and

(ii) the extent to which the action will or may reasonably be expected to reduce or manage the risk that the service will be used to solicit, access, communicate or store class 1A material or class 1B material; and

(iii) whether the proposed action is proportionate to the level of risk to online safety for end-users in Australia from the material being accessible through the service.

Note: For the object of this industry standard see section 4.

13 Index of requirements for relevant electronic services

The following table sets out the provisions of this Part applicable to providers of relevant electronic services.

Item	For this kind of relevant electronic service …	the applicable provisions of this Part are…
1	all relevant electronic services	sections 33 and 34
2	pre-assessed relevant electronic services	(a) the provisions listed in item 1 (b) sections 14 to 28, 30, 31 and 37
3	closed communication relevant electronic services	(a) the provisions listed in items 1 and 2 (b) section 35
4	dating services	(a) the provisions listed in items 1 and 2 (b) sections 32, 35 and 38

Item	For this kind of relevant electronic service …	the applicable provisions of this Part are…
5	enterprise relevant electronic services	(a) the provisions listed in item 1 (b) section 14 and subsection 38(1)
6	gaming services with communications functionality	(a) the provisions listed in items 1 and 2 (b) subsection 38(2)
7	gaming services with limited communications functionality	the provisions listed in item 1
8	open communication relevant electronic services	(a) the provisions listed in items 1 and 2 (b) sections 32 and 35
9	telephony relevant electronic service	(a) the provisions listed in item 1 (b) sections 14 to 17, 24 to 28, 30, 31 and section 37
10	Tier 1 relevant electronic service	(a) the provisions listed in item 1 (b) sections 14 to 28, 30 and 31
11	Tier 2 relevant electronic service	(a) the provisions listed in item 1 (b) sections 14 to 19, 24 to 28, 30, 31 and subsection 38(2)
12	Tier 3 relevant electronic service	the provisions listed in item 1

Division 2—Compliance measures

14 Terms of use

(1) This section applies to the following:
  (a) an enterprise relevant electronic service;
  (b) a pre-assessed relevant electronic service;
  (c) a telephony relevant electronic service;
  (d) a Tier 1 relevant electronic service;
  (e) a Tier 2 relevant electronic service.

Provisions to be included in terms of use

(2) The provider of a service must include in the terms of use for the service provisions:
  (a) imposing an obligation on the account holder of the service to ensure that the service is not used, whether by the account holder, or by an end-user in Australia, to solicit, access, distribute or store class 1A material or class 1B material; and
  (b) giving rights for the provider to do any of the following if the service is used to solicit, access, distribute or store class 1A material or class 1B material:
    (i) suspend the provision of the service to a specified end-user of the service for a specified period;
    (ii) impose specified restrictions on the use of the service by a specified end-user of the service for a specified period;
    (iii) terminate the agreement for the provision of the service.

Enforcement of terms of use

(3) If the provider of a relevant electronic service becomes aware of a breach of the obligation mentioned in paragraph (2)(a), the provider must enforce its contractual rights in respect of the breach in an appropriate way that is proportionate to the extent of the harm to the online safety of Australians that may reasonably be expected to flow from the breach.

(4) In proceedings in respect of a contravention of subsection (3), the provider bears the evidential burden of establishing:
  (a) the action it took to enforce the rights; and
  (b) that the action that it took was appropriate and proportionate, as referred to in subsection (3).

Note: For appropriate action see also section 12.

15 Notification of child sexual exploitation material and pro-terror material

(1) This section applies to the following:
  (a) a gaming service with limited communication functionality;

(b) a pre-assessed relevant electronic service;
(c) a telephony relevant electronic service;
(d) a Tier 1 relevant electronic service; and
(e) a Tier 2 relevant electronic service.

(2) If the provider of a service:
(a) identifies child sexual exploitation material, or pro-terror material, on the service; and
(b) believes in good faith that the material affords evidence of a serious and immediate threat to the life or physical safety of a person in Australia;
the provider must, as soon as practicable, report the matter to an enforcement authority, or otherwise as required by law.

(3) If the provider of a service:
(a) identifies child sexual exploitation material on the service; and
(b) believes in good faith that the material is not known child sexual exploitation material;
the provider must, as soon as practicable, notify an organisation of a kind referred to in paragraph (b) of the definition of known child sexual exploitation material in subsection 6(1).

(4) If the provider of a service:
(a) identifies pro-terror material on the service; and
(b) believes in good faith that the material is not known pro-terror material;
the provider must, as soon as practicable, notify an organisation that verifies material as pro-terror material.

Note: See the definition of ***pro-terror material*** in subsection 6(1).

(5) Subsections (2), (3) and (4) are in addition to any other applicable law.

16 Systems and processes for responding to breaches of terms of use or community standards: class 1A material

(1) This section applies to the following:
(a) a pre-assessed relevant electronic service;
(b) a telephony relevant electronic service;
(c) a Tier 1 relevant electronic service;
(d) a Tier 2 relevant electronic service.

(2) The provider of a service must implement systems and processes that ensure that, if the provider becomes aware that:
(a) there is or has been a breach of an obligation under the terms of use for the service in respect of class 1A material, including a breach of an obligation to comply with acceptable use policies; or
(b) there is or has been a breach, in Australia, involving the service, of community standards in respect of class 1A material;
the provider takes appropriate action to ensure that:

(c) the breach, if it is continuing, ceases; and
(d) the risk of further such breaches is minimised.

(3) Without limiting subsection (2), the systems, processes must include ones under which the provider:
(a) reviews reports by end-users of the service in Australia that class 1A materials are accessible using the service; and
(b) appropriately prioritises those reports and, if necessary, escalates them to senior management personnel of the provider for action.

17 Responding to breaches of terms of use or community standards: class 1A material

Note: For breaches in respect of class 1B material see section 25.

(1) This section applies to the following:
(a) a pre-assessed relevant electronic service;
(b) a telephony relevant electronic service;
(d) a Tier 1 relevant electronic service;
(d) a Tier 2 relevant electronic service.

(2) If the provider of a service becomes aware that:
(a) there is or has been a breach of an obligation under the terms of use for the service in respect of class 1A material, including a breach of an obligation to comply with acceptable use policies; or
(b) there is or has been a breach, in Australia, involving the service, of community standards in respect of class 1A material;

the provider must:
(c) as soon as practicable, remove the material, or cause the material to be removed, from the service unless it is not technically feasible for the provider to do so; and
(d) take appropriate action to ensure that:
(i) the service no longer permits access to or distribution of the material; and
(ii) the breach, if it is continuing, ceases; and
(iii) the risk of further such breaches is minimised.

Note: For appropriate action see section 12.

(3) Without limiting what is appropriate action, appropriate action may include exercising, in a way that is proportionate to the extent of the harm to the online safety of Australians that may reasonably be expected to flow from the breach, any of the provider's contractual rights under the terms of use for the service in relation to the breach.

Note: For contractual rights required to be included in terms of use see paragraph 14(1)(b).

(4) If the provider of a service becomes aware that an end-user in Australia of the service has breached obligations or standards mentioned in paragraph (2)(a) in

respect of child sexual exploitation material or pro-terror material, the provider must ensure that all the child sexual exploitation material or pro-terror material is removed from the service as soon as practicable after the provider becomes aware the breach.

(5) Subsection (4) does not affect paragraph (2)(c) and does not apply if it is not technically feasible for the provider to remove the material from the service.

18 Resourcing trust and safety functions

(1) This section applies to the following:
  (a) a pre-assessed relevant electronic service;
  (b) a Tier 1 relevant electronic service;
  (c) a Tier 2 relevant electronic service.

(2) The provider of a relevant electronic service must have and implement, in respect of the service, management, supervision and internal reporting arrangements to ensure that at all times the provider:
  (a) complies with the requirements of this industry standard; and
  (b) can otherwise effectively supervise the online safety of the service.

Note These arrangements may include duties and responsibilities for personnel, and systems, processes and technologies.

(3) The provider of a relevant electronic service must have, or have access to, sufficient personnel who have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this industry standard at all times.

19 Safety features and settings

(1) This section applies to the following:
  (a) a pre-assessed relevant electronic service;
  (b) a Tier 1 relevant electronic service; and
  (c) a Tier 2 relevant electronic service.

(2) Before the provider of the service makes a material change to the service, the provider must:
  (a) carry out an assessment of the kinds of features and settings that could be incorporated into the service to minimise the risk that class 1A material:
    (i) will be accessed by, or distributed to, end-users in Australia using the service; or
    (ii) will be stored on the service; and
  (b) determine, on the basis of the assessment, the most appropriate and effective features and settings for the service; and
  (c) ensure that the service as so changed incorporates at all times the features and settings so determined.

(3) Subsections (4), (5), (6) and (7) do not limit subsection (2) and apply whether or not a material change is made or proposed to the service.

Open communication relevant electronic services and Tier 1 relevant electronic services

(4) In the case of:

(a) an open communication relevant electronic service; or

(b) a Tier 1 relevant electronic service;

the provider must ensure that:

(c) if the service allows the sending of messages between end-users—it has tools and settings that allow end-users in Australia to block messages from other end-users; and

(d) if the service displays, or allows for the display of, an end-user's online status—it has tools and settings that an end-user in Australia can use to prevent the display or communication of the end-user's online status; and

(e) if the provider allows young Australian children to become account-holders or end-users of the service—it has tools and settings that prevent end-users who are over 18 from using the service to contact a young Australian child unless with the consent of the child's parent or guardian;

(f) the account of a young Australian child with the service is private by default; and

(g) the location of a young Australian child who is an end-user of the service is not available to end-users of the service unless with the consent of the child's parent or guardian.

Dating services

(5) The provider of a dating service must ensure that the tools and settings for the service:

(a) allow an end-user of the service to block messages from another end-user of the service; and

(b) do not permit a person to become an end-user of the service unless the person is registered with the service as an end-user; and

(c) do not permit a person to register with the service as an end-user unless the person provides the person's phone number, email address or other identifier.

(6) If a child in Australia becomes an end-user of a dating service, the provider of the service contravenes this subsection unless the provider had taken reasonable steps to ensure that children do not become end-users of the service.

Closed communication relevant electronic services

(7) The provider of a closed communication relevant electronic service must ensure that the settings for the service:

(a) do not permit a person to become an end-user of the service unless the person is registered with the service as an end-user; and

(b) do not permit a person to register as an end-user of the service unless the person provides the person's phone number, email address or other identifier.

Data retention

(8) The provider of a service must retain information provided as required by paragraph (5)(c) or (7)(b) for at least 2 years.

General information about tools and settings

(9) The provider of a service must provide information that explains the tools and settings provided as required by this section. The information:
(a) must be "in service", that is, not on a separate webpage to the webpage for the service; and
(b) must be easily accessible and easy to use; and
(c) must include or be accompanied by clear instructions on how to use the tools and settings.

20 Detecting and removing known child sexual abuse material

(1) This section applies to the following:
(a) a pre-assessed relevant electronic service;
(b) a Tier 1 relevant electronic service.

(2) The provider of a service must implement systems, processes and technologies that detect and identify known child sexual abuse material that:
(a) is stored on the service; or
(b) is accessible by an end-user in Australia using the service; or
(c) is being or has been distributed in Australia using the service.

Note: The systems, processes and technologies that the provider may use include hashing technologies, machine learning and artificial intelligence systems that scan for known child sexual abuse material.

(3) Subsection (2) does not require a provider to use a system, process or technology if it is not technically feasible for the provider to do so.

(4) The provider of a service must implement systems, processes and technologies that remove known child sexual abuse material from the service as soon as practicable after it is detected and identified.

(5) Subsection (4) does not require a provider to implement a system, process or technology if it is not technically feasible for the provider to do so.

(6) If it is not technically feasible for the provider to implement a particular system, process or technology for the purposes of:
(a) detecting and identifying known child sexual abuse material as required by subsection (2); or
(b) removing known child sexual abuse material as required by subsection (4);

the provider must take appropriate alternative action.

Note: For appropriate action see section 12.

(7) This section does not affect the operation of section 22.

Note 1: For technical feasibility, see section 7.

Note 2: This section does not prevent a provider from complying with legal obligations to preserve evidence of offences.

21 Detecting and removing known pro-terror material

(1) This section applies to the following:
  (a) a pre-assessed relevant electronic service;
  (b) a Tier 1 relevant electronic service.

(2) The provider of a service must implement systems, processes and technologies that detect and identify known pro-terror material that:
  (a) is stored on the service; or
  (b) is accessible by an end-user in Australia using the service; or
  (c) is being or has been distributed in Australia using the service.

Note: The systems, processes and technologies that the provider may use include hashing technologies, machine learning and artificial intelligence systems that scan for known pro-terror material.

(3) Subsection (2) does not require a provider to implement a system, process or technology if it is not technically feasible for the provider to do so.

(4) The provider of a service must implement systems, processes and technologies that remove known pro-terror material from the service as soon as practicable after it is detected and identified.

(5) Subsection (4) does not require a provider to implement a system, process or technology if it is not technically feasible for the provider to do so.

(6) If it is not technically feasible for the provider to implement a particular system, process or technology for the purposes of:
  (a) detecting and identifying known pro-terror material as required by subsection (2); or
  (b) removing known pro-terror material as required by subsection (4);

the provider must take appropriate alternative action.

Note: For appropriate action see section 12.

(7) This section does not affect the operation of section 22.

Note 1: For technical feasibility, see section 7.

Note 2: This section does not prevent a provider from complying with legal obligations to preserve evidence of offences.

22 Disrupting and deterring child sexual abuse material and pro-terror material

(1) This section applies to the following:
  (a) a pre-assessed relevant electronic service; and
  (b) a Tier 1 relevant electronic service.

(2) The provider of a service must implement systems, processes and technologies that:
  (a) effectively deter end-users of the service from using the service: and
  (b) effectively disrupt attempts by end-users of the service to use the service;

to create, offer, solicit, access, distribute, or otherwise make available, or store child sexual abuse material or pro-terror material (including known child sexual abuse material and known pro-terror material).

(3) Without limiting subsection (2), the systems, processes and technologies may include:
  (a) hashing technologies, machine learning and artificial intelligence systems that scan for known child sexual abuse material or known pro-terror material; and
  (b) systems, processes and technologies that are designed to detect key words, behavioural signals and patterns associated with child sexual abuse material.

23 Development programs

(1) This section applies to the following:
  (a) a pre-assessed relevant electronic service; and
  (b) a Tier 1 relevant electronic service.

for a calendar year if the average monthly number of active end-users of the service, in Australia, over the immediate previous financial year was 1,000,000 or more.

(2) The provider of the service must establish and implement, for the calendar year, a program of investment and development activities (***development program***) in respect of systems, processes and technologies.

Note: See also section 36.

(3) A development program must include:
  (a) investments and activities designed to develop systems, processes and technologies that enhance the ability of the provider, or of other providers of relevant electronic services:
    (i) to detect and identify child sexual abuse material or pro-terror material (including known child sexual abuse material and known pro-terror material) on the service; and
    (ii) to deter end-users of the service from using the service, and to disrupt attempts by end-users of the service to use the service, to solicit, generate, create, access, distribute or store child sexual abuse material

or pro-terror material (including known child sexual abuse material and known pro-terror material); and

(iii) to reduce the risk to the online safety of end-users in Australia in relation to synthetic material generated by artificial intelligence; and

(b) arrangements for cooperating and collaborating with other organisations in activities of the kind referred to in paragraph (a) and to enhance online safety for Australians.

(4) A development program may include arrangements for the provider to make available to other providers of relevant electronic services, or organisations engaged in promoting online safety for Australians, systems, processes and technologies of a kind referred to in paragraph (3)(a) (including making them available without charge).

(5) Examples of activities that may be part of a provider's development program include:

(a) joining industry organisations intended to address serious online harms; and

(b) working with the Commissioner to share information, intelligence, best practices and other information relevant to addressing categories of class 1A material or class 1B material that are relevant to the service; and

(c) collaborating with non-government or other organisations that facilitate the sharing of information, intelligence, best practices and other information relevant to addressing categories of class 1A or class 1B material that are relevant to the service.

(5) Examples of investments that may be part of a provider's development program include:

(a) procuring online safety systems and technologies for use in connection with the service, or enhancing online safety systems and technologies used in connection with the service; and

(b) conducting research into and development of online safety systems and technologies; and

(c) providing support, either financial or in kind, to organisations the functions of which are or include working to combat child sexual abuse, child sexual exploitation or terrorism.

Note: For paragraph (c), organisations can include universities, the CSIRO, the WePROTECT Global Alliance and the Global Internet Forum to Counter Terrorism (GIFCT).

24 Systems, processes and technologies for responding to breaches of terms of use or community standards: class 1B material

(1) This section applies to the following:

(a) a pre-assessed relevant electronic service;

(b) a telephony relevant electronic service;

(c) a Tier 1 relevant electronic service;

(d) a Tier 2 relevant electronic service.

(2) The provider of a service must implement systems, processes and technologies that ensure that, if the provider becomes aware that:

(a) there is or has been a breach, in Australia, of an obligation under for the terms of use for the service in respect of class 1B material, including a breach of an obligation to comply with acceptable use policies; or

(b) there is or has been a breach, in Australia, involving the service, of community standards in respect of class 1B material;

the provider takes appropriate action to ensure that:

(c) the breach, if it is continuing, ceases; and

(b) the risk of further such breaches is minimised.

(3) Without limiting subsection (2), the systems, processes and technologies must include ones under which the provider:

(a) reviews reports by end-users of the service in Australia that class 1B materials are accessible using the service; and

(b) appropriately prioritises those reports and, if necessary, escalates them to senior management personnel of the provider for action.

They must include operational guidance to provider personnel, including actions to be taken and time limits to be observed, in performing the provider's duties under this section.

25 Responding to breaches of terms of use or community standards: class 1B material

Note: For breaches in respect of class 1A material see section 17.

(1) This section applies to the following:

(a) a pre-assessed relevant electronic service;

(b) a telephony relevant electronic service;

(c) a Tier 1 relevant electronic service; and

(d) a Tier 2 relevant electronic service.

(2) If the provider of a service becomes aware that:

(a) there is or has been a breach of an obligation under the terms of use for the service in respect of class 1B material, including a breach of an obligation to comply with acceptable use policies; or

(b) there is or has been a breach involving the service, of community standards in respect of class 1B material;

the provider must:

(c) as soon as practicable, remove the material, or cause the material to be removed, from the service unless it is not technically feasible for the provider to do so; and

(d) take appropriate action to ensure that:

(i) the service no longer permits access to or distribution of the material; and

(ii) the breach, if it is continuing, ceases; and

(iii) the risk of further such breaches is minimised.

Note: For technical feasibility see section 7. For appropriate action see section 12.

(3) Without limiting what is appropriate action, appropriate action may include exercising any of its contractual rights under the terms of use for the service in relation to the breach.

Note: For the contractual rights required to be included in terms of use see paragraph 14(1)(b).

26 Giving information about the Commissioner to end-users in Australia

(1) This section applies to the following:
(a) a pre-assessed relevant electronic service;
(b) a telephony relevant electronic service;
(c) a Tier 1 relevant electronic service;
(d) a Tier 2 relevant electronic service.

(2) The provider of a service must ensure that information:
(a) describing the role and functions of the Commissioner; and
(b) describing how to make a complaint to the Commissioner about the service; and
(c) describing the mechanisms and processes required by section 27 for the service;

is accessible to end-users of the service in Australia at all times through a dedicated location on the internet site for the service.

27 Mechanisms for end-users and account holders to report, and make complaints about, material accessible through relevant electronic services

(1) This section applies to the following:
(a) a pre-assessed relevant electronic service;
(b) a telephony relevant electronic service;
(c) a Tier 1 relevant electronic service;
(d) a Tier 2 relevant electronic service.

(2) The provider of a service must provide a mechanism, tool or process that enables end-users in Australia to do each of the following:
(a) identify or flag material accessible through the service as:
(i) in breach of an obligation under the terms of use for the service, including an obligation to comply with acceptable use policies; or
(ii) in breach of community standards;
(b) report material referred to in paragraph (a) to the provider;
(c) make a complaint to the provider about material referred to in paragraph (a).

Note: For complaints see section 40.

(3) The tool, process or technology must be available "in service", that is, not on a separate webpage.

28 Mechanisms for end-users and account holders to make complaints about breaches of this industry standard

(1) This section applies to the following services:
  (a) a pre-assessed relevant electronic service;
  (b) a telephony relevant electronic service;
  (c) a Tier 1 relevant electronic service; and
  (d) a Tier 2 relevant electronic service.

(2) The provider must provide tools, processes or technologies that enables end-users of the service in Australia to make a complaint to the provider about the provider's compliance with this industry standard.

Note: For complaints see section 40.

(3) The tools, processes or technologies must be available "in service", that is, not on a separate webpage to the webpage for the service.

29 Requirements for tools, processes and technology required under section 27 or 28 for reports and complaints

(1) A tool, process or technology required by section 27 or 28 in respect of a report or a complaint:
  (a) must be easily accessible and easy to use; and
  (b) must include or be accompanied by clear instructions on how to use them; and
  (c) must enable the person making the report or complaint to specify the harm associated with the material to which the report or complaint relates.

(2) A provider must ensure that the identity of a person who makes a report or a complaint under section 27 or 28 (the ***first end-user***) is not accessible, directly or indirectly, by any other end-user of the service without the express consent of the first end-user.

30 Appropriate steps to action reports

(1) This section applies to the following:
  (a) a pre-assessed relevant electronic service;
  (b) a telephony relevant electronic service;
  (c) a Tier 1 relevant electronic service;
  (d) a Tier 2 relevant electronic service.

(2) The provider of a service must document in writing its systems, processes and technologies dealing with how it responds to reports made under paragraph 27(2)(b).

(3) The provider of a service must ensure that its personnel responding to reports made under paragraph 27(2)(b) have appropriate training in and experience of the provider's policies and procedures for dealing with reports.

31 Policies and terms of use terms to be published

(1) This section applies to the following:
  (a) a pre-assessed relevant electronic service;
  (b) a telephony relevant electronic service;
  (c) a Tier 1 relevant electronic service;
  (d) a Tier 2 relevant electronic service.

(2) The provider of a service must publish:
  (a) its terms of service for the service, including its terms relating to its acceptable use policies; and
  (b) a statement setting out the community standards applicable to the service.

(3) The publication must be accessible on the website and application (if any) for the service.

(4) The publications must:
  (a) be in plain English; and
  (b) make it clear that class 1A material is not permitted on the service and describe the broad categories of material within class 1A material; and
  (c) describe the broad categories of material within class 1B material and specify the extent to which that material is not permitted on the service, or is subject to specified restrictions.

32 Dedicated section of website for online safety information

(1) This section applies to any of the following:
  (a) a closed communication relevant electronic service;
  (b) a dating service;
  (c) a gaming service with communication functionality;
  (d) an open communication relevant electronic service;
  (e) a Tier 1 relevant electronic service.

. (2) The provider of a service must ensure that the information required by section 26 and paragraph 29(1)(b), and other online safety information made available by the provider, is accessible at all times through a dedicated location "in service", that is, not on a separate webpage to the webpage for the service.

Division 3—Reporting requirements

33 Commissioner may require risk assessments and other information

(1) The Commissioner may, by notice to the provider of a relevant electronic service, require the provider to give the Commissioner any of the following documents:

(a) the most recent risk profile determination for the service;

(b) the record, as required by section 10, of the most recent risk assessment for the service;

(c) the most recent assessment under paragraph 19(2)(a) for the service;

(d) the provider's development program for a specified calendar year.

Note: For development programs see section 23.

(2) The provider must give the documents to the Commissioner within the period specified in the notice.

Note: See also section 39.

34 Reports of technical feasibility of compliance with provisions of Division 2

(1) The Commissioner may, by notice to the provider of a relevant electronic service, require the provider to give the Commissioner a report that specifies the extent to which it is technically feasible for the provider to comply with a specified provision of Division 2.

(2) If the report discloses that it is not, or has not been, technically feasible for the provider to use a system, process or technology as required by subsection 20(2) or (4), the report must specify the alternative action required by subsection 20(6).

Note: Section 20 is about known child sexual abuse material.

(3) If the report discloses that it is not, or has not been, technically feasible for the provider to use a system, process or technology as required by subsection 21(2) or (4), the report must specify the alternative action required by subsection 21(6).

Note: Section 21 is about known pro-terror material.

(4) The Commissioner may, by notice to the provider, require the report to be in a specified form. The provider must comply with the requirement.

(5) A report may relate to 2 or more services.

(6) The provider must give the report to the Commissioner within the period specified in the notice.

Note: See also section 39.

35 Notifying new features of relevant electronic services

(1) This section applies to the following:

(a) a closed communication relevant electronic service;

(b) a dating service;
(c) a gaming service with communication functionality;
(d) an open communication relevant electronic service;
(e) a Tier 1 relevant electronic service.

(2) If the provider of a service decides to add a new feature or function to the service, the provider must notify the Commissioner of the proposed change as soon as practicable after making the decision unless the provider considers, on reasonable grounds, that the proposed change will not significantly increase the risk that the service will be used to solicit, access, distribute or store class 1A material or class 1B material.

(3) If a new feature or function is added to a service, the provider of the service must notify the Commissioner of the change as soon as practicable unless the provider determines, on reasonable grounds, that the change has not significantly increased the risk that the service will be used to solicit, access, distribute or store class 1A material or class 1B material.

36 Reports on outcomes of development programs

(1) The Commissioner may, by notice to the provider of a relevant electronic service to which section 23 applied in respect of a particular calendar year, require the provider to give the Commissioner a report that specifies:
(a) the activities and investments undertaken by the provider in respect of the calendar year to implement its development program; and
(b) the outcomes of those activities and investments in terms of enhancing online safety for end-users in Australia.

(2) The Commissioner may, by notice to the provider, require the report to be in a specified form. The provider must comply with the requirement.

(4) The provider must give the report to the Commissioner within the period specified in the notice.

Note: See also section 39.

37 Annual compliance reports: pre-assessed relevant electronic services and Tier 1 relevant electronic services

(1) This section applies to the following:
(a) a pre-assessed relevant electronic service;
(b) a Tier 1 relevant electronic service.

(2) The provider of a service must, in accordance with this section, give the Commissioner a report (a ***compliance report***) for each calendar year during which the service was provided to end-users in Australia (each calendar year is a ***reporting period***).

(3) A compliance report under subsection (2) must include the following:

(a) the average number of monthly active users of the service in Australia during the reporting period to which the report relates, and how that number was worked out;

(b) for a Tier 1 relevant electronic service—details of the most recent risk assessment for the service, including about the plan and methodology required by subsection 9(1);

(c) for a pre-assessed relevant electronic service—a description of the service's functionalities and features during the reporting period and an explanation why the service is properly characterised as the relevant kind of service;

(d) details of the steps that the provider took during the reporting period to comply with the requirements of this Part;

(e) an explanation why the steps taken as mentioned in paragraph (d) were appropriate, having regard, among other things, to the features of the service during the reporting period;

(f) a statement of the extent to which it was not, during the reporting period, technically feasible for the provider to detect or remove class 1A material or class 1B material from the service, and why;

(g) the amount of child sexual exploitation material and pro-terror material that the provider removed from the service during the reporting period;

(h) details of how the child sexual exploitation material and pro-terror material that the provider removed from the service during the reporting period was detected and identified;

(i) the number of complaints made to the provider about the provider's compliance with this industry standard during the reporting period.

Note: For paragraph (g), examples include end-user reports and use of hashing technologies.

(4) The report must provide justification for the conclusions in the report.

(5) The Commissioner may, by notice to the provider, require the compliance report to be in a specified form. The provider must comply with the requirement.

(6) A compliance report may relate to 2 or more services.

(7) If information required to be included in a compliance report has otherwise been given to the Commissioner, the provider may refer to the report or notification by which it was given instead of repeating it in the compliance report.

(8) A compliance report must be given to the Commissioner within 2 months after the end of the reporting period.

Note: See also section 39.

38 Compliance and other certificates and reports required by Commissioner

Enterprise relevant electronic services

(1) The Commissioner may, by notice to the provider of an enterprise relevant electronic service, require the provider to certify that, except as specified in the

certificate, the provider has complied with section 14 during the immediate past calendar year.

Other relevant electronic services

(2) The Commissioner may, by notice to the provider of any of the following:
   (a) a closed communication relevant electronic service;
   (b) a dating service;
   (c) a gaming service with communications functionality;
   (d) a telephony relevant electronic service;
   (e) a Tier 2 relevant electronic service;

require the provider to give the Commissioner a report (in this section, a ***compliance report***) for the immediately preceding calendar year (in this section, the ***reporting period***).

(3) A compliance report under subsection (2) must include the following:
   (a) for a telephony relevant electronic service—a description of the service's functionalities and features and an explanation why the service is properly characterised as a telephony relevant electronic service;
   (b) for a Tier 2 relevant electronic service—details of the most recent risk assessment, including about the plan and methodology required by subsection 9(1);
   (c) in any case:
      (i) details of the steps that the provider took during the reporting period to comply with the requirements of Part 4;
      (ii) an explanation why the steps taken as mentioned in subparagraph (c)(i) were appropriate, having regard, among other things, to the features of the service during the reporting period;
   (f) a statement of the extent to which it was not, during the reporting period, technically feasible for the provider to detect or remove class 1A material or class 1B material from the service, and why.

(4) A compliance report under subsection (3) must provide justification for the conclusions in the report.

(5) The Commissioner may, by notice to the provider, require the compliance report to be in a specified form. The provider must comply with the requirement.

(6) A compliance report may relate to 2 or more services.

Giving certificates and reports

(7) A provider must comply with a notice under this section within 2 months after service of the notice on the provider.

Note: See also section 39.

39 Extension of reporting periods

The Commissioner may, on application, extend the period within which a provider must give the Commissioner a report, certificate or notification under this Division, and may do so before or after the period has expired.

Part 5—Miscellaneous

40 Complaint resolution arrangements

(1) This section applies to a relevant electronic service if this industry standard requires the provider to make provision in respect of complaints by end-users in Australia of the service.

(2) If a complaint in relation to the service is made by an end-user, the provider must:

(a) investigate the complaint; and

(b) notify the complainant of the outcome of the investigations and the action proposed by the provider to in consequence of the investigation.

(3) Subsection (2) does not apply if:

(a) the provider believes on reasonable grounds that the complaint was frivolous or vexatious or otherwise not made in good faith; or

(b) the matter the subject of the complaint is being investigated, or has been investigated, by the Commissioner under Division 5 of Part 3 of the Act.

41 Record-keeping requirements

(1) The section applies to all relevant electronic services.

(2) The provider of a service must keep records that set out the actions that the provider has taken to comply with this industry standard.

(3) The provider must keep the records for at least 2 years after the end of the calendar year during which the action was taken.