



Australian Government

Office of the Australian Information Commissioner

Guidelines for recognising external dispute resolution schemes under s 35A of the *Privacy Act 1988*



The Office of the Australian Information Commissioner (OAIC) was established on 1 November 2010 by the *Australian Information Commissioner Act 2010*.

All OAIC publications can be made available in a range of accessible formats for people with disabilities. If you require assistance, please [contact the OAIC](#).

Date of initial publication: September 2013

Creative Commons

With the exception of the Commonwealth Coat of Arms, and to the extent that copyright subsists in a third party, this report, its logo and front page design are licensed under a Creative Commons Attribution 3.0 Australia licence (<http://creativecommons.org/licenses/by/3.0/>).

To the extent that copyright subsists in third party quotes and diagrams it remains with the original owner and permission may be required to reuse the material.

Content from these guidelines should be attributed as: Office of the Australian Information Commissioner, *Guidelines for recognising external dispute resolution schemes under s35A of the Privacy Act 1988*.

Enquiries regarding the licence and use of the guidelines are welcome at:

Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001
Telephone: 02 9284 9800
Email: enquiries@oaic.gov.au
Web: www.oaic.gov.au

Contents

Key messages	1
Part 1 – Purpose and objectives of the guidelines	2
The purpose of these guidelines.....	2
The legislation	2
Complaint-handling for entities under the Privacy Act	3
Complaint-handling by Australian Privacy Principles entities	3
Complaint-handling by credit reporting bodies and credit providers	3
The Privacy Act process for EDR scheme recognition	3
The Information Commissioner’s objectives in recognising EDR schemes	4
Part 2: The external dispute resolution scheme benchmarks.....	7
Accessibility of an EDR scheme.....	7
The independence of the EDR scheme	8
The fairness of the EDR scheme	8
The accountability of the EDR scheme	8
The efficiency of the EDR scheme.....	8
The effectiveness of the EDR scheme.....	9
Part 3: Privacy and other considerations	10
Remedies for privacy-related complaints.....	10
Remedies in the course of settling a dispute.....	10
Remedies in the course of making a decision.....	11
Review of dispute resolution process	11
Commitment to privacy	11
Impact on credit providers.....	12
Avoiding the need for credit providers to join an additional EDR scheme	12
Ensuring that all credit providers are eligible to join a recognised EDR scheme	13
Part 4: The conditions for continuing recognition.....	14
Specified period of recognition.....	14
Specified conditions of recognition	14
Independent review	15
Reporting data on privacy-related complaints including serious or repeated interferences with privacy and systemic issues.....	15
Other general conditions	17
Part 5: The registration process for recognition of an EDR scheme	18

Schemes already recognised and/or which have a statutory basis.....	18
Other schemes	19
All schemes	19
Varying and revoking recognition	20
The Information Commissioner’s process for varying or revoking recognition	20
Transitional arrangements	21
Appendix A: DIST Benchmarks	23

Key messages

1. In developing these guidelines, the Information Commissioner acknowledges the expertise and experience of existing industry external dispute resolution (EDR) schemes, and the important role these schemes play alongside the Office of the Australian Information Commissioner (OAIC) in handling privacy complaints.
2. The Information Commissioner acknowledges that there are existing recognition mechanisms for those schemes. Particularly, the Commissioner acknowledges the importance of not unduly burdening existing schemes if their existing recognition is based on the same requirements for recognition required under the *Privacy Act 1988* (the Privacy Act).
3. Under s 35A of the Privacy Act, the Information Commissioner may recognise an EDR scheme. In order to be recognised, EDR schemes must demonstrate their accessibility, independence, fairness, accountability, efficiency and effectiveness to the Commissioner. These recognition requirements, as set out in s35A, are based on the *Benchmarks for Industry Based Customer Dispute Resolution Schemes* developed in 1997 by the then Australian Government Department of Industry, Science and Tourism. Most existing EDR schemes are required to, or do, design their operations in accordance with these benchmarks.
4. However, to be recognised under the Privacy Act, EDR schemes should also meet additional requirements that are specifically related to privacy complaints. Most existing schemes that currently handle privacy complaints will already meet these additional requirements.
5. The additional requirements for recognition of an EDR scheme under the Privacy Act involve accountability, reporting and regular reviews. Where existing schemes must meet similar requirements under a separate recognition mechanism, they can use compliance with these to demonstrate their ability to meet the requirements under these guidelines and the Privacy Act. However supplementary requirements may be required for ongoing Privacy Act recognition (see Part 3 below).
6. The detail in these guidelines will generally assist a proposed new EDR scheme:
 - which is not already recognised under another recognition scheme, and/or
 - does not have a statutory basis for their operation,in seeking recognition under the Privacy Act, and to understand the full extent of what is required for initial and ongoing recognition.

Part 1 – Purpose and objectives of the guidelines

The purpose of these guidelines

1.1 The Office of the Australian Information Commissioner (OAIC) developed these guidelines to assist external dispute resolution (EDR) schemes to understand:

- the Information Commissioner's¹ process for recognising EDR schemes
- how the Information Commissioner will assess the matters that must be taken into account when recognising an EDR scheme
- the conditions relating to privacy complaints that the Information Commissioner may require of an EDR scheme for recognition
- if necessary, how the Information Commissioner may vary or revoke an EDR scheme's recognition.

The legislation

1.2 The *Privacy Act 1988* (the Privacy Act) gives the Information Commissioner the discretion to recognise EDR schemes to handle privacy-related complaints (s 35A).²

1.3 The Privacy Act also gives the Information Commissioner the discretion to decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made, or which the Information Commissioner has accepted, if the Information Commissioner is satisfied that the act or practice:

- is being dealt with by a recognised EDR scheme (s 41(1)(dc)), or
- would be more effectively or appropriately dealt with by a recognised EDR scheme (s 41(1)(dd)).

1.4 The OAIC supports the use of EDR schemes by individuals seeking to have a privacy-related complaint resolved. Information about how and when the Information Commissioner will decide not to investigate a complaint or otherwise transfer the complaint to a recognised EDR scheme is set out in enforcement guidelines issued by the OAIC.³

1.5 The support of the OAIC for the use of EDR schemes extends to the credit reporting system, however in this context a credit provider must be a member of a recognised EDR scheme to be able to participate in the credit reporting system (s 21D(2)(a)(i) of the Privacy Act).

¹ The Australian Information Commissioner is the head of the Office of the Australian Information Commissioner, an independent statutory agency which has functions in relation to information policy and independent oversight of privacy protection and freedom of information. The Commissioner is supported by two other statutory officers: the Privacy Commissioner and the Freedom of Information Commissioner. More information about the OAIC is available at: www.oaic.gov.au.

² Note that, unless otherwise indicated, legislative references in these guidelines are to the *Privacy Act 1988*, including amendments by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

³ See the OAIC's website <www.oaic.gov.au> for Privacy Act enforcement guidelines.

Complaint-handling for entities under the Privacy Act

Complaint-handling by Australian Privacy Principles entities

1.6 An entity bound by the Australian Privacy Principles⁴ (an APP entity) must implement practices, procedures and systems to deal with privacy-related inquiries or complaints from individuals (APP 1.2).

1.7 An individual's complaint will generally follow a three-stage process:

- the individual first makes a complaint to an APP entity
- if the individual is not satisfied with the outcome offered by the APP entity, the individual may make a complaint to a recognised EDR scheme of which that APP entity is a member
- if an APP entity is not a member of a recognised EDR scheme, or the individual is not satisfied with the outcome of the EDR process, the individual may make a complaint to the Information Commissioner under s 36 of the Privacy Act.

Complaint-handling by credit reporting bodies and credit providers

1.8 The Privacy Act contains more prescriptive requirements for credit reporting bodies' and credit providers' complaint handling processes. Like APP entities, credit reporting bodies and credit providers must implement practices, procedures and systems to deal with privacy-related enquiries or complaints from individuals (ss 20B(2) and 21B(2)). In addition, Division 5 of Part IIIA of the Privacy Act sets out how credit reporting bodies and credit providers must deal with complaints about credit-related information.

1.9 A credit provider must also be a member of a recognised EDR scheme to be able to disclose information to credit reporting bodies (s 21D).

1.10 The general complaint-handling scheme for credit-related complaints is modified for credit reporting bodies and credit providers where the complaint relates to an individual's request for access to, or correction of, their credit-related information. If an individual requests access to, or correction of, their credit-related information and the request is refused, the individual may make a complaint directly to a recognised EDR scheme of which the credit reporting body or credit provider is a member, or to the Information Commissioner (s 40(1B)).

The Privacy Act process for EDR scheme recognition

1.11 The process by which the Information Commissioner exercises his or her discretion to recognise an EDR scheme is outlined in s 35A of the Privacy Act as follows:

- a) The Commissioner may, by written notice, recognise an EDR scheme for an entity or a class of entities; or for a specified purpose.

⁴ The Australian Privacy Principles (APPs) are defined in s 14 of the Privacy Act as the principles set out in Schedule 1 to the Act.

- b) In considering whether to recognise an EDR scheme, the Commissioner must take the following matters into account:
- (i) the accessibility of the EDR scheme
 - (ii) the independence of the EDR scheme
 - (iii) the fairness of the EDR scheme
 - (iv) the accountability of the EDR scheme
 - (v) the efficiency of the EDR scheme
 - (vi) the effectiveness of the EDR scheme
 - (vii) any other matter the Commissioner considers relevant.
- c) The Commissioner may:
- (i) specify a period for which the recognition of an EDR scheme is in force
 - (ii) make the recognition of an EDR scheme subject to specified conditions, including conditions relating to the conduct of an independent review of the operation of the EDR scheme; and
 - (iii) vary or revoke:
 - A. the recognition of an EDR scheme
 - B. the period for which the recognition is in force
 - C. a condition which the recognition is subject to.

1.12 In general, the Information Commissioner will recognise an EDR scheme ‘for a specified purpose’. That is, an EDR scheme will be recognised for dealing with a particular type or range of complaints, such as ‘complaints relating to an act or practice that is an interference with the privacy of an individual under ss 13-13F of the Privacy Act’.

1.13 A recognised EDR scheme is not expected to handle complaints outside its scope, or terms of reference (where applicable). The Information Commissioner will consult with an EDR scheme prior to setting the specified purpose for which the scheme is recognised.

1.14 A notice of recognition of the EDR scheme will be recorded on a register of recognised EDR schemes maintained by the OAIC on its website. This notice will include the ‘specified purpose’ for the EDR scheme’s recognition.

The Information Commissioner’s objectives in recognising EDR schemes

1.15 In exercising the discretion to recognise an EDR scheme, the Information Commissioner’s aims are to:

- simplify the resolution of privacy-related complaints for individuals
- ensure credit providers can become members of schemes (a prerequisite for credit providers to disclose credit information to a credit reporting body)
- implement Parliament’s decision to formally create a tiered complaint process in relation to privacy complaints

- increase consistency and best practice in privacy-related complaint-handling across industries
- maximise the use of specialist industry knowledge
- avoid fragmenting among multiple dispute resolution bodies of an individual's complaint, which may include a privacy and service-delivery aspect
- align the requirements for recognition as much as possible with relevant existing regulatory schemes for EDR recognition.⁵

1.16 By achieving these aims, the following outcomes for individuals, EDR schemes and the Information Commissioner's Privacy Act functions should be realised:

Outcomes for individuals

1.17 Recognising EDR schemes under the Privacy Act benefits individuals by:

- providing a free, quick and informal alternative dispute resolution process to resolve an individual's privacy-related complaint
- simplifying the complaints process where it involves multiple issues, not just a privacy aspect.

Outcomes for EDR schemes

1.18 Recognising EDR schemes under the Privacy Act benefits EDR schemes by:

- empowering EDR schemes with the ability to offer their members and individuals a dispute resolution process for complaints which include a privacy aspect that is recognised by the Privacy Act
- developing industry specific privacy compliance knowledge and enhancing privacy practices in the industry.

Outcomes for APP entities

1.19 Recognising EDR schemes under the Privacy Act can benefit APP entities by:

- facilitating the development of industry standards for complaint handling
- allowing them to demonstrate their commitment to privacy. APP entities offer customers an additional avenue for privacy-related concerns through EDR schemes, and EDR schemes offer member APP entities support and expertise in privacy-related complaint handling.

Outcomes for the Information Commissioner's Privacy Act functions

1.20 The performance of the Information Commissioner's functions under the Privacy Act will be enhanced by the recognition of EDR schemes by:

⁵ These guidelines have been most closely aligned with the Australian Securities and Investments Commission (ASIC)'s regulatory process for the registration and oversight of EDR schemes. For information on that scheme see [ASIC's Regulatory Guides 139 and 165](#).

- formally acknowledging and supporting the role that EDR schemes play in resolving privacy complaints
- providing an opportunity to increase consistency in how privacy-related complaints are dealt with across different industries
- decreasing the fragmentation of complaints across multiple dispute resolution bodies when the complaint arises from a single set of facts
- utilising existing specialist knowledge and practices in particular industry sectors to resolve complex, multifaceted disputes.

Part 2: The external dispute resolution scheme benchmarks

- 2.1 Under s 35A(2)(a) to (g) of the Privacy Act, when considering whether to recognise an EDR scheme, the Information Commissioner must take into account the accessibility, independence, fairness, accountability, efficiency and effectiveness of the EDR scheme, and any other matter the Commissioner considers relevant (for the latter see Part 3 of these guidelines).
- 2.2 The matters which the Information Commissioner must take into account are based on the benchmarks developed in 1997 by the then Department of Industry, Science and Tourism (DIST) for industry-based customer dispute resolution schemes (DIST benchmarks).⁶ These benchmarks are still considered best practice requirements. The underlying principle for each DIST benchmark is set out in **Appendix A: DIST Benchmarks** of these guidelines. DIST also identified the purpose of each benchmark and key practices that could be used to assess whether an EDR scheme meets each benchmark.
- 2.3 Outlined below is some detail about the benchmarks and key practices that will assist applicants in understanding the matters in s 35A(2)(a) to (f), which the Commissioner must take into account in considering an application for recognition. Most existing schemes will already be able to demonstrate that they meet these criteria through providing information on their existing recognition process (or their statutory basis where relevant). More information about how existing schemes can practically demonstrate they meet these criteria is outlined in Part 5 of these guidelines.

Accessibility of an EDR scheme

- 2.4 An EDR scheme can demonstrate accessibility through, for example:
- actively promoting its services to individuals
 - ensuring access to and ease of use of its services
 - generally providing its services to individuals free of charge
 - training its staff to handle complaints and to be able to explain the functions and powers of the EDR scheme in simple and clear terms
 - encouraging informal and alternative methods of dispute resolution
 - encouraging parties to only involve legal representatives if special circumstances require this expertise.

⁶ Department of Industry, Science and Tourism 1997, [Benchmarks for Industry-Based Customer Dispute Resolution Schemes](#), Department of Industry, Science and Tourism, Canberra.

The independence of the EDR scheme

2.5 An EDR scheme must be able to undertake its dispute resolution work independent of those sectors of industry that fall within its jurisdiction and provide it funding. Approaches demonstrating an EDR scheme's independence from its members may include, for example:

- establishing a governance body to oversee the EDR scheme's operation
- having a principal decision-maker responsible for deciding complaints and appropriate delegations in place
- ensuring the principal decision-maker and staff of the EDR scheme are not able to be inappropriately influenced by EDR scheme members in relation to the EDR scheme's decisions or operation
- being resourced appropriately to carry out the EDR scheme's functions
- consulting widely with relevant stakeholders in developing or changing the EDR scheme's scope.

The fairness of the EDR scheme

2.6 An EDR scheme's procedures should accord procedural fairness and should be transparent to all parties to a complaint. An EDR scheme can achieve fairness through, for example:

- basing decisions on what is fair and reasonable in all the circumstances
- affording procedural fairness to all parties using the EDR scheme
- requiring EDR scheme members to provide all information that they hold, relevant to a complaint, to the EDR scheme
- ensuring the EDR scheme appropriately respects the confidentiality of information provided to it for the purposes of resolving complaints.

The accountability of the EDR scheme

2.7 Accountability ensures continuing public confidence in the EDR scheme. It also assists EDR scheme members to assess and improve their personal information handling practices. An EDR scheme can publicly account for its operations by, for example, publishing in accessible formats:

- notable decisions
- the EDR scheme's rules
- an annual report.

The efficiency of the EDR scheme

2.8 An EDR scheme operates efficiently when, for example, it:

- deals only with complaints within its scope

- does not handle complaints that have been dealt with, or are being dealt with, by another appropriate dispute resolution forum
- keeps track of complaints
- regularly reviews its performance.

The effectiveness of the EDR scheme

2.9 An EDR scheme can demonstrate its effectiveness by, for example:

- ensuring the scope of the EDR scheme is clear and sufficient to deal with privacy-related complaints
- ensuring systems are in place to refer complaints about the EDR scheme to an overseeing entity (where applicable)
- having mechanisms in place to bind EDR scheme members to the rules and decisions of the EDR scheme.

Part 3: Privacy and other considerations

3.1 Under s 35A(2)(g) of the Privacy Act, the Information Commissioner must take into account any other matter he or she considers relevant when considering whether to recognise an EDR scheme.

3.2 Matters considered relevant for this purpose are related to an EDR scheme's ability to handle privacy-related complaints and the benefits of recognising EDR schemes that operate under existing regulatory regimes. These include:

- a) the remedies the EDR scheme can provide for privacy-related complaints
- b) the EDR scheme's commitment to privacy
- c) the impact on credit providers of not recognising a particular EDR scheme.

Remedies for privacy-related complaints

3.3 The Information Commissioner will consider whether the EDR scheme has appropriate powers to provide individuals with sufficient remedies for their privacy-related complaints. The Information Commissioner will consider the extent to which those remedies are generally consistent with remedies that may be:

- available to the individual if the individual complained to the Information Commissioner rather than the EDR scheme
- awarded if the individual complained to the Information Commissioner rather than the EDR scheme.

3.4 An EDR scheme should be able to provide information to the parties on appropriate remedies to assist them in their attempt to settle their dispute. The EDR scheme should be open and transparent about the types of remedies it can order when making a decision.

Remedies in the course of settling a dispute

3.5 The aim of an alternative dispute resolution process, such as conciliation, negotiation or mediation, is to reach a settlement that will resolve the complaint of the individual. In general, a resolution that the parties reach together, rather than having imposed upon them, leads to a greater commitment to the outcome and to a greater likelihood of compliance.

3.6 In resolving the complaint, the parties can reach an arrangement that includes any remedy that is lawful. The facilitator overseeing the alternative dispute resolution process should consider and provide information to parties on the range of remedies that could be pursued.

3.7 Remedies for privacy-related complaints may include one or more of the following:⁷

- an apology to the individual
- being provided with access to information or charges for access being reduced
- compensation
- correction or amendment of a record
- extra services or services at reduced costs
- the respondent entity improving systems or procedures, including changed or upgraded security arrangements for personal information
- privacy notices being changed or updated
- staff training for the respondent entity.

Remedies in the course of making a decision

3.8 An EDR scheme's decision-maker should have the power to make binding decisions on the respondents. Those powers should include the ability to provide remedies that are generally consistent with the declarations available to the Information Commissioner when he or she makes a determination under s 52 of the Privacy Act.

Review of dispute resolution process

3.9 An EDR scheme may conduct an internal review of the outcome if an individual is not satisfied with the EDR scheme's alternative dispute resolution process or decision. EDR schemes should conduct internal reviews where appropriate.

3.10 Where internal review is not conducted, an EDR scheme should provide an individual that is not satisfied with the outcome of the EDR process in relation to their complaint, with information about making a complaint to the Information Commissioner. Where internal review is conducted, an EDR scheme should provide information about making a complaint to the Information Commissioner to an individual that is not satisfied with the outcome of the internal review.

Commitment to privacy

3.11 The Information Commissioner notes that some EDR schemes may not be APP entities and so will not be subject to the APPs in the Privacy Act (although they may be covered by state or territory laws for handling personal information). Where EDR schemes are not bound by the APPs the Commissioner will, before recognising the EDR scheme, require them to have a privacy policy to explain how the scheme manages the personal information it collects, and the information flows associated with that information. Without limiting the contents of the

⁷ *Privacy Complaints Practice and Procedure Manual, 2011*,
http://www.oaic.gov.au/publications/other_operational/complaint_handling_manual_april2011.html

privacy policy, the policy should include information similar to that required by APP 1.4.⁸

3.12 If there are significant differences between the way the EDR scheme handles personal information and the requirements of the Privacy Act, the EDR scheme should draw this to the Commissioner's attention and outline those differences.

3.13 An EDR scheme must take such steps as are reasonable in the circumstances to make its privacy policy available free of charge, in an appropriate and readily accessible form.

Impact on credit providers

3.14 A credit provider must be a member of a recognised EDR scheme to be able to disclose credit information to a credit reporting body (s 21D(2)(a)(i)). Therefore the Information Commissioner will consider the impact on credit providers of not recognising a particular EDR scheme. For the credit reporting system to function as intended, at least one EDR scheme that credit providers can join must be recognised.

Avoiding the need for credit providers to join an additional EDR scheme

3.15 Credit providers, as defined in s 6G of the Privacy Act, include entities from a range of industries including banks, utility providers and telecommunication service providers. The Information Commissioner is aware that many credit providers are already members of EDR schemes. In some instances, other regulatory regimes require those credit providers to be members of particular EDR schemes.⁹

3.16 The Information Commissioner is mindful of the burden that would be imposed on credit providers if they were required to join an additional EDR scheme for the purposes of participating in the credit reporting system. The Information Commissioner is also mindful that privacy-related complaints are often part of a wider complaint about the provision of goods or services. If a credit provider was required to join an EDR scheme in relation to privacy-related complaints, but was a member of a different EDR scheme in relation to other complaints, there would be the risk of fragmenting the individual's complaints between two or more EDR schemes. This may make resolving disputes more difficult, impose extra costs on industry, and lead to confusion for individuals making privacy-related complaints. This outcome will be avoided where possible.

⁸ See 'Guidelines for Australian Privacy Principle 1 - Open and transparent management of personal information' for further guidance on what is required for a privacy policy.

⁹ For example, s 47 of the *National Consumer Credit Protection Act 2009* requires credit licensees to be members of an EDR scheme approved by the Australian Securities and Investments Commission.

Ensuring that all credit providers are eligible to join a recognised EDR scheme

- 3.17 The Information Commissioner is aware that EDR schemes may limit their membership to certain entities for legitimate reasons. The Information Commissioner is mindful that if a credit provider is not eligible to join any recognised EDR scheme the credit provider will be unable to participate in the credit reporting system.
- 3.18 While it is not the responsibility of the Information Commissioner to ensure that a recognised EDR scheme exists for each credit provider to join, the Information Commissioner will take this consideration into account. The Information Commissioner may, for example, conditionally recognise an EDR scheme as outlined in Part 4 of these guidelines.

Part 4: The conditions for continuing recognition

4.1 Under s 35A(3) of the Privacy Act, the Information Commissioner may:

- a) specify a period for which the recognition of an EDR scheme is in force
- b) make the recognition of an EDR scheme subject to specified conditions, including conditions relating to the conduct of an independent review of the operation of the EDR scheme.

4.2 The Information Commissioner will generally recognise EDR schemes on an on-going basis. However, the recognition will be subject to specified conditions with which the EDR scheme must continue to comply for the recognition to remain in force.

Specified period of recognition

4.3 In some circumstances, the Information Commissioner may recognise an EDR scheme for a specified period of time, and review the EDR scheme's recognition at the end of that period. These circumstances include when:

- the EDR scheme's role in the regulatory framework for the industry is changing
- the EDR scheme is at risk of having its recognition revoked under another regulatory regime, or
- the EDR scheme is going to cease operating, or cease to handle the types of complaints that the EDR scheme is recognised for.

4.4 The Information Commissioner may also recognise an EDR scheme for a specified period of time, or subject to additional conditions where the EDR scheme substantially meets the Commissioner's requirements for recognition, but requires more time to fully implement the necessary changes to meet those requirements. In such circumstances, the Commissioner may recognise the EDR scheme in a limited capacity only, to minimise the risk of fragmenting the handling of complaints related to the same goods and services that involve both privacy and service delivery related aspects.

Specified conditions of recognition

4.5 The Information Commissioner will make the recognition of all EDR schemes subject to the following specified conditions (as discussed further below). The EDR Scheme must:

- provide the Commissioner with an independent review of the EDR scheme at least once every five years
- meet the Commissioner's requirements for reporting serious or repeated interferences with privacy and systemic issues and data on privacy-related complaints

- comply with other general conditions appropriate for handling privacy-related complaints.

Independent review

- 4.6 Regular and independent review of an EDR scheme's performance is a key practice to indicate an EDR scheme's efficiency. The Information Commissioner may make the recognition of an external dispute resolution scheme subject to specified conditions, including the conduct of an independent review of the operation of the EDR scheme (s 35A(3)(b)).
- 4.7 The Information Commissioner requires a recognised EDR scheme to commission an independent review of the EDR scheme's privacy-related complaint-handling, operations and procedures at least once every five years. This review can be conducted as part of a broader independent review of the EDR scheme.
- 4.8 The EDR scheme must consult the Information Commissioner about the terms of the review before the review commences.
- 4.9 The review should be undertaken in consultation with relevant stakeholders (such as the EDR scheme's members and relevant consumer groups) and should examine:
- the EDR scheme's ongoing ability to satisfy the matters the Information Commissioner must take into account when recognising an EDR scheme as outlined in Parts 2 and 3 of these guidelines
 - the EDR scheme's ongoing ability to satisfy the conditions of the EDR scheme's recognition as outlined in Part 4 of these guidelines
 - how satisfied individuals and EDR scheme members are with the operation of the scheme
 - any other relevant matters, including matters the Commissioner considers relevant following notification by the EDR scheme to the Commissioner of the independent review's terms of reference.
- 4.10 The EDR scheme should provide relevant parts of the report of the review to the Information Commissioner. The Commissioner may publish relevant parts of the report on its website after consultation with the EDR scheme.

Reporting data on privacy-related complaints including serious or repeated interferences with privacy and systemic issues

- 4.11 The Information Commissioner considers that systematic monitoring and regular reporting of privacy-related complaints by EDR schemes will improve industry practice and help reduce the risk of privacy-related issues occurring.
- 4.12 In general, the objectives of requiring EDR schemes to monitor and report privacy-related complaint information is to:
- improve the privacy practices of members of the EDR schemes

- ensure high-risk issues or conduct are identified and addressed in a timely manner
- provide the Information Commissioner with data from a range of EDR schemes so that he or she can examine whether there are systemic issues across a range of sectors
- assist the Commissioner to target community and industry awareness programs about appropriate personal information handling practices.

4.13 If an EDR scheme believes these conditions should be tailored to its membership and complaints profile, then the EDR scheme should outline these matters to the Information Commissioner when it applies for recognition.

General reporting on privacy-related complaints

4.14 EDR schemes should provide privacy-related complaint information to the OAIC on an annual basis for inclusion in the OAIC's Annual Report.¹⁰ The information should be placed in its appropriate context – for example, by explaining why there may have been an increase in privacy-related complaints compared to the previous year.

4.15 Where possible EDR schemes should provide information about:

- a) the number of privacy-related complaints received in the financial year
- b) the average time taken to resolve privacy-related complaints in the financial year
- c) for privacy-related complaints finalised in the financial year, statistical information about:
 - the outcomes (eg conciliations, withdrawals)
 - the nature of remedies agreed through conciliation, or by decision (eg compensation, apology, staff training)¹¹
- d) any systemic privacy-related issues or trends identified in the financial year.

Monitoring and reporting serious or repeated interferences with privacy and systemic issues¹²

4.16 To register an EDR scheme, the Information Commissioner requires the EDR scheme to have processes in place to identify, through complaints and other

¹⁰ In order to meet the OAIC's annual report publication deadline EDR schemes will be requested to provide this information by 31 July for the preceding 12 month period ending on 30 June.

¹¹ Please see Chapter Six of the OAIC annual report 2011-12 for a list of categories under which an EDR scheme may report outcomes and remedies for privacy-related complaints- <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201112/>

¹² Systemic privacy issues are issues that are inherent in the overall way an industry operates and has a wider effect than just the immediate parties to a complaint. Systemic privacy issues arise from the overall conduct of entities or the way an industry operates. Systemic privacy issues may be identified by an EDR scheme from a single complaint or from multiple complaints. At other times, systemic privacy issues may only be identifiable once the Commissioner has collected data from a number of EDR schemes.

information received by the scheme, serious or repeated interferences with privacy¹³, and systemic privacy issues of the EDR scheme's members. An EDR scheme should also have processes in place to refer serious or repeated interferences with privacy and systemic privacy issues to relevant EDR scheme members for response and action, or to the industry regulator where applicable and appropriate (e.g. ACMA or ASIC).

4.17 Serious or repeated interferences with privacy and systemic privacy issues should be reported to the Information Commissioner when an EDR scheme has confirmed that such events have occurred. See Annexure 1 for more details on reporting serious or repeated interferences with privacy and systemic privacy issues.

4.18 If EDR scheme members do not appropriately rectify serious or repeated interferences with privacy or systemic issues within a reasonable period of time, the Information Commissioner may investigate the act or practice of an entity on the Commissioner's own initiative under Part V of the Privacy Act. The Commissioner may also choose to investigate the act or practices of an entity under certain circumstances, such as when it is in the public interest to do so.

4.19 Serious or repeated interferences with privacy can attract a civil penalty under s 13G of the Privacy Act. More information in relation to serious or repeated interferences with privacy is available on the [OAIC's website](#).

Other general conditions

4.20 In addition to conditions requiring regular independent reviews and regular reports regarding privacy-related complaints, an EDR scheme's recognition will be subject to the following general conditions. An EDR scheme must:

- accept relevant privacy-related complaints referred to the EDR scheme by the Information Commissioner, provided the complaint falls within the EDR scheme's scope or terms of reference (see paragraph 1.12 of these guidelines)¹⁴
- advise the Commissioner if there is an anticipated change to the EDR scheme that is relevant to its role as a recognised EDR scheme under the Privacy Act. For example, if the EDR scheme is going to cease operating, cease to be the EDR scheme for a specific industry, or is at risk of having its recognition revoked under another regulatory regime
- advise the Commissioner if the EDR scheme anticipates it will no longer be able to satisfy any of the matters in Parts 2, 3 or 4 of these guidelines
- inform the Commissioner if there is an anticipated change to the EDR scheme's ability to deal with privacy-related complaints

¹³ See the OAIC's 'Enforcement guidelines' for further guidance on serious or repeated interferences with privacy (<www.oaic.gov.au>).

¹⁴ Details of how the Commissioner will refer and transfer complaints to EDR schemes are detailed in the enforcement guidelines issued by the OAIC (see <www.oaic.gov.au>).

- have a process in place for handling privacy-related complaints of an EDR scheme member where that member ceases to carry on a business, becomes insolvent or is liquidated.

Part 5: The registration process for recognition of an EDR scheme

5.1 An EDR scheme seeking to be recognised should make a written application which includes all relevant documentation. Relevant documentation, for this purpose, will be dependent on whether the EDR scheme is already recognised under another recognition scheme or has a statutory basis for its operation.

5.2 The Information Commissioner will publish an EDR scheme's application, and any relevant documentation, on the OAIC website in the interests of transparency of the application process, *after consultation with the EDR scheme*. Furthermore, any information provided as part of an EDR scheme's application may be subject to obligations under the *Freedom of Information Act 1982*.

Schemes already recognised and/or which have a statutory basis

5.3 Existing EDR schemes that are already recognised under another recognition scheme, and/or which have a statutory basis for their operation, should include in their application:

- a covering letter addressed to the Information Commissioner requesting recognition
- details of previous recognition under another regulatory EDR recognition scheme and any conditions attached to that recognition (this will be met by a copy of any certificate of recognition) and/or the statutory basis for their operation
- documentation that demonstrates adherence with the DIST benchmarks, or, in lieu of such documentation, a declaration from the Chief Executive Officer (or equivalent) that the EDR scheme works or will work within these benchmarks
- an outline of how the EDR scheme will implement the additional privacy-related requirements set out in these guidelines
- the relevant parts of the most recent independent review of the EDR scheme (if any)
- if relevant:
 - how and why conditions for reporting data on privacy-related complaints should be tailored to the EDR scheme's membership and complaints profile
 - details of communications with members, potential members, consumer representatives and other regulatory bodies regarding the EDR scheme's application to be recognised by the Information Commissioner.

Other schemes

5.4 Other EDR schemes, not already recognised under another recognition system or not having a statutory basis should include the following in their application:

- a covering letter addressed to the Information Commissioner
- detailed and specific information about how the EDR scheme satisfies or will satisfy the matters in Parts 2, 3 and 4 of these guidelines
- if relevant, information around any other EDR scheme currently operating within the industry that the new scheme intends to join, and information regarding why a new EDR scheme is required to enter that industry, including the benefit to individuals.
- membership details of the EDR scheme and details of any membership conditions
- the articles of association, constitution and terms of reference, where applicable, and details of any proposals to amend these
- if relevant, details of the membership of, and appointment to, an overseeing body
- the most recent independent review of the EDR scheme (if any)
- the EDR scheme's most recent annual report
- a summary of the complaints information the EDR scheme collects
- if relevant – how and why conditions for reporting data on privacy-related complaints should be tailored to the EDR scheme's membership and complaints profile
- details of any consultation with members, potential members, consumer representatives and other regulatory bodies about the EDR scheme being recognised by the Commissioner and any outstanding issues from those consultations.

All schemes

5.5 The Information Commissioner may request further documents and information from the EDR scheme during the registration process. The Commissioner may also consider information provided by industry, consumer representatives and other interested stakeholders. If the Commissioner considers material provided other than by the EDR scheme, the EDR scheme will have an opportunity to respond.

5.6 The Information Commissioner will provide a written notice of recognition to each EDR scheme that is recognised. The notice will be a public document available on a register of recognised EDR schemes maintained by the OAIC on its website and will contain details of:

- the entity, class of entities or purpose for which the EDR scheme is recognised
- the period for which recognition of the EDR scheme is in force
- any specified conditions under which the EDR scheme is recognised.

5.7 The EDR scheme should notify its members in writing that it has been recognised.

5.8 In order for the recognition to remain in force, the EDR scheme must continue to satisfy the matters in Parts 2, 3 and 4 of these guidelines and any additional conditions imposed by the Information Commissioner.

Varying and revoking recognition

5.9 Under s 35A(3)(c) of the Privacy Act, the Information Commissioner may vary or revoke:

- a) the recognition of an EDR scheme
- b) the period for which the recognition is in force
- c) a condition to which the recognition is subject.

5.10 Matters that may cause the Information Commissioner to vary or revoke an EDR scheme's recognition include, but are not limited to:

- if the EDR scheme has not complied with a condition of its recognition, for instance:
 - it has been more than five years since the EDR scheme was last independently reviewed, as discussed in paragraph 4.7 of these guidelines
 - the EDR scheme is unable to satisfy the Commissioner it meets the matters in Parts 2, 3 and 4 of these guidelines
 - a persistent failure to provide annual reports to the Commissioner and / or to report any serious or repeated interferences with privacy or systemic issues
 - the EDR scheme's ability to deal with privacy-related complaints changes without notification to the Information Commissioner
- an independent review finds the EDR scheme does not meet one or more of the matters in Parts 2, 3 and 4 of these guidelines
- the EDR scheme is no longer adequately funded to have the capacity to handle privacy-related complaints
- conditions previously imposed by the Commissioner on the EDR scheme's recognition are no longer warranted.

The Information Commissioner's process for varying or revoking recognition

5.11 The Information Commissioner will provide a notice of intention in writing to the recognised EDR scheme about changes that are proposed to be made to its recognition, and provide reasons for the proposed changes. The Commissioner may also request that the EDR scheme consult its members about the proposed changes.

- 5.12 The EDR scheme will be given a specified period to respond to the Commissioner's notice and provide any information that it would like the Commissioner to take into account.
- 5.13 In addition to the information provided by the EDR scheme, the Commissioner may consider information provided by industry, consumer representatives and other interested stakeholders as part of this process. The EDR scheme will be given an opportunity to respond to the information and evidence provided by other stakeholders.
- 5.14 In considering whether to vary or revoke an EDR scheme's recognition, the Information Commissioner will consider whether:
- the EDR scheme is able or willing to demonstrate the matters the Commissioner must take into account under s 35A(2) of the Privacy Act, as detailed in Parts 2 and 3 of these guidelines
 - the EDR scheme is able or willing to comply with conditions imposed on its recognition by the Commissioner under s 35A(3) of the Privacy Act, as detailed in Part 4 of these guidelines
 - the EDR scheme is able or willing to comply with any other conditions the Commissioner considers appropriate
 - varying or revoking the EDR scheme's recognition would have an impact on its members and on individuals who have existing complaints lodged with the EDR scheme.
- 5.15 An EDR scheme may also write to the Information Commissioner requesting that its terms of recognition be varied or revoked. The request should be made in writing and give reasons for its request, including details of any consultation the EDR scheme has had with its members and any supporting documentation.
- 5.16 If the Information Commissioner considers varying or revoking an EDR scheme's recognition to be appropriate he or she will provide a written notice with reasons outlining why the decision was made. The notice will set out the changes to the EDR scheme's recognition and date the change takes effect. The EDR scheme will be required to inform its members in writing of the variation or revocation of its recognition.
- 5.17 The notice and reasons will be publicly available and will be made available on the OAIC's website and the EDR scheme's details on the OAIC's register of recognised EDR schemes will be updated.

Transitional arrangements

- 5.18 If the Information Commissioner varies or revokes an EDR scheme's recognition, the EDR scheme may be required to take steps to ensure existing privacy-related complaints it is processing are dealt with appropriately. For example, that individuals with complaints being handled by the EDR scheme are

notified of the revocation or variation to the EDR scheme's recognition and are notified of their right to lodge their complaint with the Commissioner or, if relevant, another EDR scheme.

Appendix A: DIST Benchmarks

Accessibility	The EDR scheme makes itself readily available to customers by promoting knowledge of its existence, being easy to use and having no cost barriers.
Independence	The decision-making process and administration of the EDR scheme are independent from EDR scheme members.
Fairness	The EDR scheme produces decisions which are fair and seen to be fair by observing the principles of procedural fairness, by making decisions on the information before it and by having specific criteria upon which its decisions are based.
Accountability	The EDR scheme publicly accounts for its operations by publishing its decisions and information about complaints and highlighting any systemic industry problems.
Efficiency	The EDR scheme operates efficiently by keeping track of complaints, ensuring complaints are dealt with by appropriate process or forum and regularly reviewing its performance.
Effectiveness	The EDR scheme is effective by having appropriate and comprehensive terms of reference and periodic independent review of its performance.

Excerpt from the Benchmarks for Industry-Based Customer Dispute Resolution Schemes, published by the then Department of Industry, Science and Tourism in 1997.

Annexure 1 - Reporting serious or repeated interferences with privacy and systemic privacy issues

- 1.1 This annexure provides advice to recognised EDR schemes regarding the practices and procedures for reporting serious or repeated interferences with privacy and systemic privacy issues, as required by para 4.17 of the Guidelines.
- 1.2 Whilst the phrases ‘systemic privacy issue’, ‘serious interference with privacy’ and ‘repeated interference with privacy’ are not defined in the Privacy Act, they are explained in the OAIC’s [Privacy regulatory action policy and Guide to privacy regulatory action, as outlined below](#).

Systemic privacy issues

- 1.3 A systemic privacy issue is a privacy issue that may have implications or an effect beyond a particular incident. This may occur where an incident indicates there is an ongoing or underlying problem with practices, procedures or systems that relate to privacy compliance, adherence to those practices, procedures or systems, or with attitudes to privacy compliance.
- 1.4 A privacy issue may be systemic within a single entity, or more broadly within an industry sector. A systemic privacy issue may be identified from an incident which is brought to an EDR’s attention by a single complaint or multiple complaints of a similar nature against one or several of its members.

Serious or repeated interference with privacy

- 1.5 Whether an interference with privacy is ‘serious’ is an objective question that will reflect what a reasonable person would consider serious. This means that what is considered a serious interference with privacy may vary and evolve over time as technology and community expectations regarding privacy protections change.
- 1.6 ‘Repeated interference with privacy’ means that an entity has interfered with the privacy of an individual or individuals on two or more separate occasions. These repeated interferences with privacy could arise from:
 - the same act or practice done on two or more occasions
 - different acts or practices done on two or more occasions.

Procedure for reporting incidents

- 1.7 Where an EDR scheme becomes aware of a potential systemic privacy issue or serious or repeated interference with privacy by one of its members, it should notify that member of the issue with a view to confirming:
 - whether or not the systemic privacy issue or serious or repeated interference with privacy has occurred

- the action and response (if any) by the member.
- 1.8 If an EDR scheme confirms that a serious or repeated interference with privacy or a systemic privacy issue has occurred, the EDR schemes must report it to the OAIC. The EDR scheme can report all confirmed serious or repeated interference with privacy or a systemic privacy issues to the OAIC on a quarterly basis, using the reporting template below, via the EDR scheme mailbox (EDRschemes@oaic.gov.au). EDR schemes may report a serious or repeated interference with privacy or a systemic privacy issue more frequently where they consider that it would be appropriate for it to be brought to the OAIC's attention sooner.
- 1.9 To the extent possible, the EDR schemes should include the following information in its quarterly report to the OAIC:
- a. the details of the serious or repeated interference with privacy, or systemic privacy issue
 - b. the identity of the reported EDR member(s)
 - c. the action taken by the reported EDR member(s), and also by the EDR scheme, in response to the serious or repeated interference with privacy, or systemic issue
 - d. any resolution or outcome to the serious or repeated interference with privacy, or systemic privacy issue.
- 1.10 An EDR scheme should continue to report quarterly on a serious or repeated interference with privacy, or systemic privacy issue, while the EDR scheme is still engaging with the EDR scheme member(s) in relation to the issue.
- 1.11 Upon receipt of a quarterly report from an EDR scheme, the OAIC will provide an acknowledgement email to the EDR scheme. The OAIC will consider whether:
- a. the OAIC has received any other complaints against, or is otherwise aware of potential breaches by, the reported EDR member(s)
 - b. Whether similar complaints have been made against, or similar breaches have occurred by, other entities.
- 1.12 If necessary, the OAIC may request further information from an EDR scheme about the report. The OAIC will treat any information it receives from EDR schemes as confidential.
- 1.13 The OAIC will report de-identified, aggregated statistics in its Annual Report on the serious or repeated interferences with privacy, or systemic privacy issues.

Possible further action to be taken by OAIC on reported incidents

- 1.14 The OAIC recognises the role and independence of EDR schemes in the three-tiered complaints handling process under the *Privacy Act 1988*. This

includes an EDR scheme's expertise in dealing with complaints within its jurisdiction, and an EDR scheme's pre-existing relationship with its members. As such, the OAIC's preference is for EDR schemes to handle systemic privacy issues or serious or repeated interferences with privacy against its members at the first instance.

- 1.15 However, in certain circumstances, the OAIC may decide to take additional regulatory action against the reported EDR scheme member. The decision whether or not to take this further action will be done in accordance with OAIC's [privacy regulatory action policy](#). The OAIC will consult the EDR scheme in deciding to undertake further regulatory action.

Template for reporting serious or repeated interferences with privacy and systemic privacy issues

EDR scheme	Name of scheme
Reported EDR scheme member	Name of reported entity
Is this a serious or repeated interference with privacy, or a systemic privacy issue	List whether serious or repeated interference, or alternatively a systemic issue
Details of the serious/repeated or systemic issue	Outline the details of the reported issue
Any action taken by the reported EDR member	What actions did the reported entity take in response to the issue?
Any action taken by the reported EDR scheme	What actions did the EDR scheme take in response to the issue?
Any resolution	If applicable, has the issue been resolved/ what was the final outcome or result?