Chapter 12:

Australian Privacy Principle 12 —

Access to personal information

Version 1.1, July 2019

OAIC

Contents

Key points 3
What does APP 12 say? 3
'Holds' 4
Access to 'personal information' 4
Verifying an individual's identity 5
Giving access under APP 12 — general processing requirements 5
Giving access under APP 12 — further processing requirements for agencies 6
Refusing to give access under APP 12 — agencies 7
Authority to refuse access under the FOI Act 7
Required or authorised to refuse access under another Act 8
Refusing to give access under APP 12 — organisations 9
Giving access would pose a serious threat to the life, health or safety of any individual or to public health or public safety 9
Giving access would have an unreasonable impact on the privacy of other individuals 10
The request for access is frivolous or vexatious 10
The information requested relates to an existing or anticipated legal proceeding 11
Giving access would prejudice negotiations between the organisation and the individual 11
Giving access would be unlawful 11
Denying access is required or authorised by law or a court/tribunal order 12
Giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct 12
Giving access would be likely to prejudice an enforcement related activity conducted by, or on behalf of, an enforcement body 13
Giving access would reveal evaluative information in connection with a commercially sensitive decision-making process 13
APP 12 minimum access requirements 14
Difference with access requirements applying to agencies under FOI Act 14
Timeframe for responding to a request for access under APP 12 — agencies 14
Timeframe for responding to a request for access under APP 12 — organisations 15
How access is to be given under APP 12 15
Giving access by other means 15
Giving access through an intermediary 16
Access charges under APP 12 — agencies 16
Access charges under APP 12 — organisations 16
Giving written notice where access is refused, or not given in the manner requested under APP 12 17

Key points

- APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request.
- APP 12 also sets out other requirements in relation to giving access, including how access is to be given and when access can be refused. There are separate grounds on which agencies and organisations may refuse to give access.
- APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be provided with access to information, including, for agencies, the Freedom of Information Act 1982 (FOI Act) that provides a right of access to information held by agencies.

What does APP 12 say?

12.1 An APP entity that holds personal information about an individual must, on request, give that individual access to the information (APP 12.1). The grounds on which access may be refused differ for agencies and organisations.

12.2 APP 12 also sets out minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused.

12.3 APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be given access to information. In particular, APP 12 does not prevent an APP entity from giving access to personal information under an informal administrative arrangement,[1] provided the minimum access requirements stipulated in APP 12 have been met.

12.4 For agencies, APP 12 operates alongside the right of access in the FOI Act. The FOI Act provides individuals with a right of access to documents held by most Australian Government agencies,[2] including documents containing personal information.[3]

12.5 Some paragraphs in this Chapter are only relevant to agencies or to organisations:

- paragraphs only for agencies: 12.22–12.24; 12.25–12.32; 12.66; 12.76
- paragraphs only organisations: 12.33–12.62; 12.67; 12.77–12.81

[1] For information about administrative access schemes, see OAIC, Administrative Access, OAIC website <https://www.oaic.gov.au>.

[2] The FOI Act is expressed to apply separately to Ministers' offices in respect of 'an official document of a Minister' (s 48). APP 12 also applies to Ministers' offices: see the discussion of 'APP entity' in Chapter B (Key concepts), and the Privacy Act s 7(1)(d),(e).

[3] The Australian Information Commissioner has issued Guidelines (the FOI Guidelines) under s 93A of the FOI Act to which regard must be had for the purposes of performing a function, or exercising a power, under that Act. The FOI Guidelines are available at OAIC website <https://www.oaic.gov.au>.

‘Holds’

12.6 APP 12 only applies to personal information that an APP entity ‘holds’. An APP entity ‘holds’ personal information ‘if the entity has possession or control of a record that contains the personal information’ (s 6(1)).

12.7 The term ‘holds’ extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information. In these circumstances, the entity must comply with APP 12 by giving the individual access (unless an exception applies). It cannot simply refer the individual to the third party that has physical possession. However, the individual has a separate right to request access from the third party, if the third party is an APP entity.

12.8 An agency that has placed a record of personal information in the care of the National Archives of Australia, or in the custody of the Australian War Memorial, is considered to be the agency that holds the record for the purposes of the Privacy Act (s 10(4)).

12.9 Upon receiving a request for access, an APP entity should search the records that it possesses or controls to assess whether the requested personal information is contained in those records. For example, an entity may search hard copy records and electronic databases and make enquiries of staff or contractors with relevant knowledge. A discussion with the individual may assist the entity to locate the information.

12.10 The term ‘holds’ is discussed in more detail in Chapter B (Key concepts).

Access to ‘personal information’

12.11 APP 12 requires an APP entity to provide access to ‘personal information’. It does not provide a right of access to other kinds of information. ‘Personal information’ is defined in s 6(1) as ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not, and
- whether the information or opinion is recorded in a material form or not’

12.12 Personal information of one individual may also be personal information of another individual. For example:

- information in a marriage certificate may be personal information of both parties to the marriage
- an opinion may be personal information of both the subject and the giver of the opinion

12.13 APP 12 requires an APP entity to provide access to all of an individual’s personal information it holds, even if that information is also the personal information of another individual, unless a ground to refuse access applies. The grounds are discussed below, and include the ground that giving access would have an unreasonable impact on the privacy of another individual. ‘Personal information’ is discussed in more detail in Chapter B (Key concepts).

12.14 As to other requested information that is not personal information:

- If the APP entity is an organisation, it could consider whether the person has a right of access to that information under other legislation. If not, the organisation may make a

discretionary decision either to grant access to that other information or to refuse access.

- If the entity is an agency, it could consider whether access to that information can be granted under the FOI Act, or on an administrative basis. Before refusing access to that other information, the agency should advise the individual to consider making the request under the FOI Act.

Verifying an individual's identity

12.15 An APP entity must be satisfied that a request for personal information under APP 12 is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, as a legal guardian or authorised agent. If an entity gives access to the personal information of another person, this could constitute a disclosure, which may not comply with APP 6 (see Chapter 6).

12.16 It would generally be impracticable for an APP entity to deal with an anonymous request for personal information. However, it may be practicable to deal with a pseudonymous request, for example, where the individual has previously transacted under that pseudonym, can establish their identity as that individual and the request for access relates to information about that pseudonymous identity (see Chapter 2 (APP 2)).

12.17 The steps appropriate to verify an individual's identity will depend on the circumstances. In particular, whether the individual is already known to or readily identifiable by the APP entity, the sensitivity of the personal information and the possible adverse consequences for the individual of unauthorised disclosure. The minimum amount of personal information needed to establish an individual's identity should be sought. Where possible, the personal information should be sighted rather than copied or collected for inclusion in a record. For example, in a face-to-face dealing with an individual, an entity may be able to record that an identity document was sighted without copying the document. In a telephone contact it may be adequate to request information that can be checked against records held by the entity. An entity that collects personal information to verify an individual's identity should consider the requirement in APP 11.2, to take reasonable steps to destroy or de-identify personal information no longer needed for any purpose for which it may be used or disclosed (unless an exception applies) (see Chapter 11 (APP 11)).

Giving access under APP 12 — general processing requirements

12.18 APP 12 requires that personal information be given to an individual 'on request'. APP 12 does not stipulate formal requirements for making a request, or require that a request be made in writing, or require the individual to state that it is an APP 12 request.[4]

12.19 It is open to an APP entity to provide access to personal information on an informal basis, provided the minimum access requirements in APP 12 are met. The access requirements in APP 12 relate to response times (see paragraphs 12.66–12.67 below), how access is to be given (see paragraphs 12.68–12.75 below), access charges (see paragraphs 12.76–12.81 below), and providing a written notice, including the reasons for the refusal, if access is

[4] This differs from the formal requirements relating to requests for access to documents under Part III of the FOI Act. See Part III of the FOI Act and Part 3 of the FOI Guidelines, OAIC website <https://www.oaic.gov.au>.

refused (see paragraphs 12.82–12.87 below). These are only the minimum requirements. An entity should endeavour to provide access in a manner that is as prompt, uncomplicated and inexpensive as possible.

12.20 An APP entity is required by APP 1.4(d) to state in an APP Privacy Policy 'how an individual may access personal information about the individual' (see Chapter 1 (APP 1)). An APP entity is also required by APP 5.2(g) to take reasonable steps to notify an individual, or ensure they are aware, of the fact that the entity's APP Privacy Policy contains information about how the individual may access their personal information held by the entity.

12.21 If an APP entity wishes an individual to follow a particular procedure in requesting access to their personal information, the entity could publish that procedure and draw attention to it, for example, by providing a link in the entity's APP Privacy Policy and on the entity's website homepage to the access procedure, to an online request form, or to an online portal that enables an individual to access their personal information. However, an entity cannot require an individual to follow a particular procedure, use a designated form or explain the reason for making the request. Any recommended procedure should be regularly reviewed to ensure that it is flexible and facilitates rather than hinders access.

Giving access under APP 12 — further processing requirements for agencies

12.22 Agencies should ensure that APP 12 access procedures are integrated with FOI Act procedures. The FOI Act sets out comprehensive rules about requesting and providing access to documents held by most Australian Government agencies, including documents containing personal information, and resolving access disputes. An important FOI requirement is that an agency has a duty to take reasonable steps to assist an individual to make an access request that complies with the FOI Act access requirements (FOI Act, s 15(3)). That means an agency could refer to the FOI Act in the agency's APP Privacy Policy and, in appropriate circumstances, draw the FOI Act to an individual's attention. Agencies should also consider providing this information through an 'Access to information' link on the agency's website homepage.[5]

12.23 Agencies are not required to advise individuals to request personal information under the FOI Act rather than under an administrative arrangement or by relying on APP 12. As explained in the FOI Guidelines,[6] agencies should consider establishing administrative access arrangements that operate alongside the FOI Act and that provide easier and less formal means for individuals to obtain access to government information, including personal information. Providing access to personal information under an administrative arrangement will fulfil an agency's obligation under APP 12 to provide access upon request, provided the arrangement meets the minimum access requirements in APP 12.

12.24 In some circumstances it may be preferable for an agency to suggest that an individual make an access request under the FOI Act:

- An FOI access request can relate to any document in the possession of an agency (FOI Act, s 15(1)) and is not limited to personal information held in an agency record (APP 12.1).

[5] See OAIC, Guidance for Agency Websites: 'Access to Information' Web Page, OAIC website <https://www.oaic.gov.au>.

[6] See OAIC, FOI Guidelines, Part 3, OAIC website <https://www.oaic.gov.au>. See also OAIC, Administrative Access, OAIC website <https://www.oaic.gov.au>.

- The FOI Act contains a consultation process for dealing with requests for documents that contain personal or business information about a person other than the requester (FOI Act, ss 27, 27A).
- An applicant who applies for access under the FOI Act can complain to the Information Commissioner about an action taken by an agency under that Act (FOI Act, s 70) (complaint mechanisms under the Privacy Act are discussed in paragraph 12.30 and 12.87 below).
- An applicant who is refused access under the FOI Act has a right to apply for internal review or Information Commissioner review of the access refusal decision (FOI Act, ss 54, 54L).

Refusing to give access under APP 12 — agencies

12.25 An agency is not required by APP 12 to give access to personal information if the agency is required or authorised to refuse access to that information by or under:

- the FOI Act (APP 12.2(b)(i))
- any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents (APP 12.2(b)(ii))

12.26 The meaning of 'required or authorised' is discussed in Chapter B (Key concepts). In summary, an agency is 'required' to refuse access by an Act that prohibits the disclosure of the personal information; and an agency is 'authorised' to refuse access by an Act that authorises or confers discretion on the agency to refuse a request for access to the personal information.

Authority to refuse access under the FOI Act

12.27 The FOI Act lists several grounds on which an agency can refuse a request under the Act for access to documents. An agency may rely on any of those grounds to refuse access under APP 12. It is nevertheless open to an agency not to rely on any such ground and to provide access upon request, unless disclosure is prohibited, for example, by a secrecy provision.[7]

12.28 The grounds on which an access request can be declined under the FOI Act include:[8]

- a document is an exempt document under Part IV, Division 2 of the FOI Act, for example, the document is a Cabinet document, is subject to legal professional privilege, contains material obtained in confidence, or a secrecy provision applies
- a document is a conditionally exempt document under Part IV, Division 3 of the FOI Act, for example, the document contains deliberative matter, or disclosure of the document would involve the unreasonable disclosure of personal information about another

[7] The same discretionary principle applies under the FOI Act. Section 3A of the FOI Act provides that it does not limit any power of an agency to publish or grant access to information under other legislative or administrative schemes.

[8] The Australian Information Commissioner has issued guidelines (the FOI Guidelines) under s 93A of the FOI Act to which regard must be had for the purposes of performing a function, or exercising a power, under that Act. See OAIC, FOI Guidelines, OAIC website <https://www.oaic.gov.au>.

person and it would be contrary to the public interest to release the document at that time

- the individual is not entitled to obtain access to a document of the kind requested, for example, the document is available for purchase from an agency (FOI Act, ss 12, 13)
- providing access in the terms requested by a person would substantially and unreasonably divert an agency's resources from its other operations (s 24AA)
- processing a person's request would require an agency to disclose the existence or non-existence of a document, where that would otherwise be exempt information (s 25)

12.29 The FOI Act specifies consultation processes that may apply to requests made under that Act, for example, where a 'practical refusal reason' may apply (FOI Act, s 24) to the request, or where a requested document contains a third party's personal or business information (FOI Act, ss 27, 27A). An agency is not required to undertake any of those consultation processes before refusing access on any of those grounds under APP 12. This is required only if the person decides to make a request under the FOI Act.

12.30 A decision to refuse access under APP 12.2(b)(i) (on one of the FOI grounds listed above) is a decision made under the Privacy Act, not the FOI Act. As required by APP 12.9, the agency must provide the individual with a written notice that sets out the reasons for the refusal and the complaint mechanisms available to the individual (see paragraph 12.87 below). The individual may have a right to complain to the Information Commissioner under the Privacy Act. After investigation, the Commissioner may make a determination that the agency has failed to comply with APP 12 and require, for example, that the agency give access (Privacy Act, s 52). However, the individual will not have a right to seek internal review or Information Commissioner review under the FOI Act.

Required or authorised to refuse access under another Act

12.31 APP 12.2(b)(ii) provides that an agency is not required to give access to personal information if it is required or authorised to refuse to give access by another Act that provides for access by persons to documents. An example is a statutory secrecy provision that requires or authorises that access be refused in certain circumstances.

12.32 A further example is that the National Archives of Australia (NAA) is authorised to refuse access to certain 'exempt records' under the Archives Act 1983 (the Archives Act). The Archives Act provides that the NAA must make available for public access Commonwealth records in the open access period that are in the care of the NAA and that are not exempt records (s 31 of the Archives Act). The categories of exempt records include information whose disclosure would constitute a breach of confidence, would involve the unreasonable disclosure of information relating to the personal affairs of any person, or would unreasonably affect a person adversely in relation to his or her business, financial or professional affairs (s 33 of the Archives Act).[9]

[9] For further information about the National Archives of Australia's obligation to make available Commonwealth records for public access, see National Archives of Australia website <www.naa.gov.au>.

Refusing to give access under APP 12 — organisations

12.33 APP 12.3 lists ten grounds on which an organisation can refuse to give access to personal information. It is nevertheless open to an organisation not to rely on any such ground and to provide access upon request, unless disclosure is prohibited. Before relying on any of these grounds an organisation should consider whether redacting some information would enable access to be provided (for example, redacting personal information about another person).

12.34 The grounds, which are considered separately below, are:

- the organisation reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety (APP 12.3(a))
- giving access would have an unreasonable impact on the privacy of other individuals (APP 12.3(b))
- the request for access is frivolous or vexatious (APP 12.3(c))
- the information relates to existing or anticipated legal proceedings between the organisation and the individual, and would not be accessible by the process of discovery in those proceedings (APP 12.3(d))
- giving access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations (APP 12.3(e))
- giving access would be unlawful (APP 12.3(f))
- denying access is required or authorised by or under an Australian law or a court/tribunal order (APP 12.3(g))
- the organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation's functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter (APP 12.3(h))
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 12.3(i))
- giving access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process (APP 12.3(j))

Giving access would pose a serious threat to the life, health or safety of any individual or to public health or public safety

12.35 The phrase, 'serious threats to the life, health or safety of any individual, or to public health or public safety' is discussed in Chapter C (Permitted general situations).

12.36 An example of where this ground might apply is a healthcare provider having reasonable grounds to believe that giving an individual access to their personal information may cause that person significant distress or lead to self-harm or harm to another person.

Giving access would have an unreasonable impact on the privacy of other individuals

12.37 This ground may apply where the record of personal information that an individual has requested contains personal information of another individual. As noted above (paragraph 12.12), a record of an individual's opinions or views (for example, a referee comment) may be personal information of that individual.[10]

12.38 Before relying on this ground an organisation must be satisfied that giving access would have 'an unreasonable impact' on the privacy of another. Factors that may be relevant in deciding that issue include:

- the nature of the personal information about the other individual. For example, if the personal information is of a sensitive or confidential nature it may be unreasonable to provide it to others.
- the reasonable expectation of the other individual about how that personal information will be handled (this should be assessed objectively and on the basis that the other individual may not have special knowledge of the industry or activity involved). For example, if both individuals were present when the personal information was collected, there may be a reasonable expectation that each individual could later access the personal information.
- the source of the personal information. For example, if the individual requesting access provided the personal information about the other individual, access may not have an unreasonable impact on that person.
- whether the personal information of another individual could be redacted from the record provided to the individual requesting access.
- whether access could be provided through an intermediary (see paragraphs 12.72–12.75 below).
- whether the other individual consents to access being given to the individual requesting access.

12.39 In applying this ground, an organisation may consult the other individual about whether giving access would have an unreasonable impact on their privacy. The view expressed by that individual may be relevant but not determinative. However, before consulting another individual, an organisation should consider whether doing so poses a privacy risk for the individual seeking access.

The request for access is frivolous or vexatious

12.40 A request should not be refused on this ground unless there is a clear and convincing basis for deciding that a request is frivolous or vexatious. It is not a sufficient basis, for example, that a request would cause inconvenience or irritation to an organisation.

12.41 The following are given as examples of requests that may be treated as frivolous or vexatious:

[10] For further discussion of where giving access would have an unreasonable impact on the privacy of other individuals, see Smallbone v New South Wales Bar Association [2011] FCA 1145 (6 October 2011).

- Repeated requests for access to personal information that has already been provided to the requester.
- A request that contains offensive or abusive language, or that does not appear to be a genuine request for personal information.
- A repeat request for personal information that an organisation has earlier explained to an individual it does not hold, has been destroyed, or cannot be located after a reasonable search.
- A request made for the apparent purpose of harassing or intimidating the staff of an organisation, or interfering unreasonably with its operations.

The information requested relates to an existing or anticipated legal proceeding

12.42 This ground applies where legal proceedings between the individual and the organisation are underway or anticipated, and the information would not be accessible by the process of discovery in those proceedings. A legal proceeding is anticipated if there is a real prospect of proceedings being commenced, as distinct from a mere possibility.

Giving access would prejudice negotiations between the organisation and the individual

12.43 This ground applies where giving access would prejudice negotiations between the organisation and the individual by revealing the intentions of the organisation in relation to the negotiations. The negotiations may be current or reasonably anticipated.

12.44 Examples of where this ground might apply is an organisation negotiating:

- a claim brought by an individual for compensation (for example, for negligence or wrongful dismissal), and releasing the personal information requested by the individual may reveal the organisation's strategy to settle or defend the claim
- a sponsorship arrangement with an individual, and releasing the personal information requested by the individual may reveal the organisation's strategy in relation to negotiating the arrangement

12.45 This exception applies only to personal information that would prejudice negotiations, and not to all information relevant to the negotiations. Access should be provided to other personal information that is requested, unless another exception applies.

Giving access would be unlawful

12.46 'Unlawful activity' is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. Examples of unlawful activity include criminal offences, unlawful discrimination, and trespass.

12.47 Examples of where this ground might apply are where giving access would be a breach of legal professional privilege, a breach of confidence or a breach of copyright.

Denying access is required or authorised by law or a court/tribunal order

12.48 The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in Chapter B (Key concepts). This ground applies where an Australian law or court or tribunal order forbids the disclosure of information; or a law or order authorises or confers discretion on an organisation to refuse a request from an individual for access to their personal information. (There is overlap between this ground and the preceding ground 'giving access would be unlawful'.)

12.49 An example of where this ground might apply is a court order providing that an organisation is not required to provide personal information to an individual who is in the care of or is undergoing treatment by the organisation.

Giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct

12.50 There are a number of separate elements to this ground.

12.51 First, an organisation must have reason to suspect that unlawful activity or misconduct of a serious nature has been, is being or may be engaged in. The term 'unlawful activity' is not defined in the Privacy Act. The core meaning is activity that is criminal, illegal or prohibited or proscribed by law, and can include unlawful discrimination or harassment, but does not include breach of a contract. Examples of unlawful activity include criminal offences, unlawful discrimination, and trespass.

12.52 Misconduct is defined in s 6(1) to include 'fraud, negligence, default, breach of trust, breach of duty, breach of discipline or any other misconduct in the course of duty'. An added requirement of this ground is that the misconduct is 'serious' in nature. This excludes minor breaches or transgressions.

12.53 The organisation must have 'reason to suspect' the unlawful activity or serious misconduct has been, is being or may be engaged in. This is a different and lesser standard to 'reasonably believes', which is used in some other APPs (see Chapter B (Key concepts)). There should nevertheless be a reasonable basis for the suspicion. It is the responsibility of the organisation to be able to justify its reasonable basis for the suspicion.

12.54 The suspected unlawful activity or serious misconduct must relate to the organisation's functions or activities. As discussed in Chapter 3 (APP 3), an organisation's functions or activities include current, proposed and support functions and activities.

12.55 Lastly, giving access must be likely to prejudice the organisation in taking appropriate action in relation to the suspected unlawful activity or serious misconduct. The proposed action may include investigation of the activity or misconduct, or reporting it to the police or another relevant person or authority. There should again be a reasonable basis for this expectation of prejudice. For example, in some instances giving an individual access would not prejudice the taking of appropriate action, but would allow the individual to provide further information relevant to the suspected unlawful activity.

12.56 An example of where this ground might apply is where giving access to the requested personal information would reveal that, covertly but lawfully, an organisation is

investigating suspected misconduct of a client and disclosure would prejudice the covert investigation.

Giving access would be likely to prejudice an enforcement related activity conducted by, or on behalf of, an enforcement body

12.57 'Enforcement body' is defined in s 6(1) as a list of specific bodies. The list includes Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect the public revenue or to impose penalties or sanctions. Examples of Commonwealth enforcement bodies are the Australian Federal Police, the Australian Crime Commission, Customs, the Integrity Commissioner,[11] the Immigration Department,[12] the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and AUSTRAC.

12.58 'Enforcement related activity' is also defined in s 6(1). It includes the prevention, detection, investigation and prosecution or punishment of criminal offences and intelligence gathering activities.

12.59 The terms 'enforcement related activity' and 'enforcement body' are discussed in Chapter B (Key concepts).

12.60 An example of where this ground might apply is an enforcement body asking an organisation not to give an individual access to certain personal information, as doing so would be likely to reveal the existence of a criminal investigation or interfere with preparation for court proceedings.

Giving access would reveal evaluative information in connection with a commercially sensitive decision-making process

12.61 This ground applies if giving access would reveal 'evaluative information' generated within an organisation in connection with a commercially sensitive decision-making process. An example of evaluative information is a score card weighting system and score card result. The ground applies only to the evaluative information, and not to personal information on which a decision was based.[13]

12.62 APP 12.10 provides that if an organisation refuses to give access to personal information under this ground, its written notice explaining the reasons for refusal may include an explanation for the commercially sensitive decision. This may include explaining the reasons for the decision and giving a copy of the personal information that informed the decision. For discussion of the requirement to give a written notice refusing access, see paragraphs 12.82–12.87 below.

---

[11] 'Integrity Commissioner' is defined in s 6(1) as having the same meaning as in the Law Enforcement Integrity Commissioner Act 2006.

[12] 'Immigration Department' is defined in s 6(1) as the Department administered by the Minister administering the Migration Act 1958.

[13] See also C v Insurance Company [2006] PrivCmrA 3 (1 February 2006).

APP 12 minimum access requirements

12.63 APP 12 sets out minimum access requirements that must be met when an APP entity receives a request from an individual for access to their personal information. The access requirements relate to the response time, how access is to be given, access charges and giving a written notice, including the reasons for refusal, if access is refused.

12.64 An individual may complain under s 36 to the Information Commissioner about the failure of an APP entity to comply with any of the APP 12 minimum access requirements. The Commissioner will not investigate a complaint if the person has not first raised the matter with the entity complained about, unless it was not appropriate to require that as a first step (s 40(1A)). When investigating a complaint, the OAIC will initially attempt to conciliate the complaint (s 40A), before considering the exercise of other complaint resolution powers (s 52).

Difference with access requirements applying to agencies under FOI Act

12.65 The APP 12 minimum access requirements and the Privacy Act complaint and review mechanisms differ in important respects from those applying to agencies in relation to requests for information received under the FOI Act.[14] For example, the FOI Act requires an agency to acknowledge receipt of an FOI request within 14 days, and to make a decision on the request within 30 calendar days. The processing period can be extended with the agreement of the applicant, to enable an agency to consult a third party, or with the approval of the Information Commissioner for complex and voluminous requests.[15] If an agency fails to make a decision within the statutory processing period (including an authorised extension) the agency is deemed to have made a decision refusing access. The applicant may then apply for internal review or Information Commissioner review, although the OAIC can extend the time for an agency to make a decision on the request. The FOI Act also contains special requirements on charges, the form of access and statements of reasons.

Timeframe for responding to a request for access under APP 12 — agencies

12.66 APP 12.4(a)(i) provides that an agency must 'respond' to a request for access within 30 calendar days. The 30 day time period commences on the day after the day the agency receives the request. The agency must respond by giving access to the personal information that is requested, or by notifying its refusal to give access. If this is impracticable (for example, there is a justifiable need to clarify the scope of an individual's request, or to locate and assemble the requested information, or to consult a third party), the agency is expected to contact the individual to explain the delay and provide an expected timeframe for finalising the request. These are matters the Information Commissioner may examine if a complaint is made about an agency's failure to comply with the timeframe in APP 12.4(a).

[14] The circumstances in which an individual may apply to the Administrative Appeals Tribunal for review of a decision of the Information Commissioner are set out in s 96.

[15] See OAIC, Extension of Time for Processing Requests, OAIC website <https://www.oaic.gov.au>.

Timeframe for responding to a request for access under APP 12 — organisations

12.67 APP 12.4(a)(ii) provides that an organisation must respond 'within a reasonable period after the request is made'. As with agencies, an organisation must respond by giving access to the personal information that is requested, or by notifying its refusal to give access. Factors that may be relevant in deciding what is a reasonable period include the scope and clarity of a request, whether the information can be readily located and assembled, and whether consultation with the individual or other parties is required. However, as a general guide, a reasonable period should not exceed 30 calendar days.

How access is to be given under APP 12

12.68 An APP entity must give access to personal information in the manner requested by the individual, if it is reasonable and practicable to do so (APP 12.4(b)). The manner of access may, for example, be by email, by phone, in person, hard copy, or an electronic record.

12.69 Factors relevant in assessing whether it is reasonable and practicable to give access in the manner requested by an individual include:

- the volume of information requested. For example, it may be impracticable to provide a large amount of personal information by telephone.
- the nature of the information requested. For example, it may be impracticable to give access to digitised information in hard copy and it may be unreasonable to give access to information of a highly sensitive nature by telephone if the APP entity cannot sufficiently verify the individual's identity over the telephone.
- any special needs of the individual requesting the information. For example, it may be reasonable to give information in a form that can be accessed via assistive technology where this meets the special needs of the individual.

Giving access by other means

12.70 APP 12.5 applies where an APP entity refuses to give access to personal information under APP 12 on a permitted ground, or refuses to give access in the manner requested by the individual. The entity must take reasonable steps to give access in a way that meets the needs of the entity and the individual. This should be done within 30 calendar days where practicable.

12.71 The APP entity is expected to consult the individual to try to satisfy their request.[16] The following are given as examples of alternative manners of access that may meet the needs of the entity and the individual, and in particular result in more rather than less personal information being provided to an individual:

- deleting any personal information for which there is a ground for refusing access and giving the redacted version to the individual
- giving a summary of the requested personal information to the individual
- giving access to the requested personal information in an alternative format

[16] Explanatory memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 87.

- facilitating the inspection of a hard copy of the requested personal information and permitting the individual to take notes
- facilitating access to the requested personal information through a mutually agreed intermediary (see paragraphs 12.72–12.75 below)

Giving access through an intermediary

12.72 APP 12.6 provides that, without limiting APP 12.5, 'access may be given through the use of a mutually agreed intermediary'.

12.73 The role of an intermediary is to enable an individual to be given access to their personal information and to have the content of that information explained, where direct access would otherwise be refused. An example is an organisation refusing direct access under APP 12.3(a) on the reasonable belief that access may lead the individual to self-harm, but deciding that access through an intermediary may not pose a similar threat. The role of the intermediary in conveying or explaining the information to the individual will need to be tailored to the nature of the information and any instructions given by the APP entity to the intermediary.

12.74 The intermediary must be acceptable to both the APP entity and the individual. In seeking an individual's agreement to use an intermediary, an entity should clearly explain the process and the type of access that will be provided through this process. Depending on the nature of the personal information to which access is sought, the intermediary may need particular skills or knowledge. For example, an intermediary may need to be a qualified health service provider if used to give access to health information.

12.75 If an individual does not agree to the use of an intermediary, or agreement cannot be reached on whom to use as the intermediary, the APP entity must still take reasonable steps to give access through another manner that meets the needs of the entity and the individual.

Access charges under APP 12 — agencies

12.76 An agency cannot impose upon an individual any charge for providing access to personal information under APP 12 (APP 12.7). This includes:

- a charge for the making of the request to access personal information
- a charge for giving access to requested personal information, such as charges for copying costs, postage costs and costs associated with using an intermediary

Access charges under APP 12 — organisations

12.77 An organisation cannot impose upon an individual a charge for the making of the request to access personal information.

12.78 An organisation may, however, impose a charge for giving access to requested personal information, provided the charge is not excessive (APP 12.8). Items that may be charged for include:

- staff costs in searching for, locating and retrieving the requested personal information, and deciding which personal information to provide to the individual
- staff costs in reproducing and sending the personal information

- costs of postage or materials involved in giving access
- costs associated with using an intermediary (see paragraphs 12.72–12.75 above)

12.79 Whether a charge is excessive will depend on the nature of the organisation, including the organisation's size, resources and functions, and the nature of the personal information held. The following charges may be considered excessive:

- a charge that exceeds the actual cost incurred by the organisation in giving access
- a charge associated with obtaining legal or other advice in deciding how to respond to an individual's request
- a charge for consulting with the individual about how access is to be given
- a charge that reflects shortcomings in the organisation's information management systems. An individual should not be disadvantaged because of the deficient record management practices of an organisation

12.80 An organisation should also consider waiving, reducing or sharing any charge that may be imposed, so that the charge is not excessive. In determining the amount to charge, an organisation should consider:

- the organisation's relationship with the individual
- any known financial hardship factors claimed by the individual
- any known adverse consequences on the individual if they do not get access to the personal information

12.81 A charge by an organisation for giving access must not be used to discourage an individual from requesting access to personal information. To the extent practicable, an organisation should advise an individual in advance if a charge may be imposed, and the likely amount of the charge. The individual should be invited to discuss options for altering the request to minimise any charge. This may include options for giving access in another manner that meets the needs of the entity and the individual (see APP 12.5 and paragraphs 12.70–12.71 above). Any charge that is imposed should be clearly communicated and explained before access is given.

Giving written notice where access is refused, or not given in the manner requested under APP 12

12.82 APP 12.9 provides that if an APP entity refuses to give access, or to give access in the manner requested by the individual, the entity must give the individual a written notice setting out:

- the reasons for the refusal, except to the extent that it would be unreasonable to do so, having regard to the grounds for refusal
- the complaint mechanisms available to the individual, and
- any other matters prescribed by regulations made under the Privacy Act

12.83 The reasons for refusal should explain, where applicable:

- that the entity does not hold the requested personal information
- the ground of refusal. For example, if the entity is required or authorised by an Australian law to refuse access, notice should include the name of that law and, if practicable, could include the provision relied upon.

- that access cannot be given in the manner requested by the individual, and the reason why
- that the steps necessary to give access in a way that meets the needs of the entity and the individual under APP 12.5 are not reasonable in the circumstances

12.84 The notice could, in addition, set out any steps that may be taken by the individual that would mean that access would not be refused, for example, by re-framing or narrowing the scope of the individual's request.

12.85 APP 12.10 additionally provides that, where an organisation relies on the commercially sensitive decision ground in APP 12.3(j), the written notice may provide an explanation for the commercially sensitive decision (see paragraphs 12.61–12.62 above).

12.86 An APP entity is not required to explain the ground of refusal to the extent that it would be unreasonable to do so. This course should be adopted only in justifiable circumstances. Examples for organisations include that an explanation may prejudice action by an organisation to respond to unlawful activity (APP 12.3(h)); may prejudice enforcement action by an enforcement body (APP 12.3(i)). An example for agencies is that this would reveal the existence of a document whose existence an agency would be entitled to neither confirm nor deny under s 25 of the FOI Act.

12.87 The description of the complaint mechanisms available to an individual should explain the internal and external complaint options, and the steps that should be followed. In particular, the individual should be advised that:

- a complaint should first be made in writing to the APP entity (s 40(1A))
- the entity should be given a reasonable time (usually 30 days) to respond
- a complaint may then be taken to a recognised external dispute resolution scheme of which the entity is a member (if any), and
- lastly, a complaint may be made to the Information Commissioner (s 36)