Guide on Applying Exceptions

1. Legal Framework and Overview of Principles

The right to information is recognised as a fundamental human right, both under international law and in Article 28 F of the Indonesian Constitution. This right is implemented by Law 14/2008 on Public Information Disclosure. Article 2 of Law 14/2008 establishes the key principles regarding the disclosure of public information:

a. Public information shall by default be in nature open and accessible to the public information.
b. Exceptions should be interpreted strictly and narrowly.
c. The procedure to obtain public information should be quick, inexpensive, and straightforward.
d. Information may be withheld only in accordance with the legislation, which mandates the application of a harm test and a public interest test. Information will only be withheld if the harm that will result from its release outweighs the public interest in disclosure.

These principles illustrate the default obligation on public authorities to facilitate open access to all information, and the fact that exceptions to access should be narrowly interpreted and limited in scope. Information can only witheld after the consequential harm and public interest tests have been applied. The consequential harm test involves assessing whether disclosure of the information will cause harm to one of the protected interests listed in the law. The public interest test involves balancing the general public interest in disclosure and the specific public interest in disclosure of the information, on the one hand, against the potential harm to the protected interest that would result from disclosure, on the other.

2. Decision-making Processes

The responsibility to respond to requests for access to information falls on the PPID, an official who is responsible for the storage, management and provision of information in public bodies.[1]

Upon receiving a request, the first step for the PPID is to locate the information. Where the information is clearly uncontroversial and the information officer has access to the information, he or she should simply provide it directly to the requester. In some cases, particularly if the public body not yet established the List of Public Information, the PPID may have difficulty findhing information which is responsive to the request. In that case, he or she may have to forward the request to the working level official who is responsilbe for that area of work within the public authority.

Once the relevant information has been located, the next step is to apply the test for determining whether the information should be disclosed. There are three basic components to the test:

[1] Article 1 (9) Law 14/2008.

1) The information must relate to a legitimate aim listed in the law;
2) Disclosure must threaten to cause substantial harm to that aim; and
3) The harm to the aim must be greater that the public interest in having the information.

First, the PPID should determine whether the information relates to any of the protected interests listed in Article 17 of Law 14/2008. If none of these interests are engaged, the PPID should immediately release the information. If a protected interest is engaged, the PPID should move on to the consequential harm test, as spelled out in Article 17 of Law 14/2008. If it is unclear to the PPID whether disclosure of the information may cause harm, the PPID may consult with the working level official within the public authority who is responsible for managing the information. In some cases, the working level official may need to consult with more senior colleagues so as to be able to assess the wider implications of releasing the informations, either in terms of harm or public interest considerations. If no harm is likely to result from the release of the information, the PPID should immediately release the information. However, before concluding that harm is likely to result, the PPID should consider whether the potential for harm can be nullified by blacking out the problematic words or sections, which will allow them to release the remainder of the document.

If the PPID finds a likelihood of harm, the next step is to apply the public interest test. If the public interest test weighs in favour of disclosure, the information should be immediately released. If the public interest test weighs in favour of withholding the information, then and only then can the PPID refuse to release the information. In the event of a refusal, the PPID should inform the requester of the reasons for the refusal and provide him or her with information about the appeal mechanisms which are available.

3. Consequential Harm Test

The consequential harm test is a procedure that should be performed by the PPID to determine whether certain information is exempt. This test is set out in Article 17 of Law 14/2008. This test is not an empirical test but an assessment of the logical consequences that will occur if information is disclosed.

The underlying rational is that the right to access information is a human right and if no harm will result from the disclosure of certain information, then there is no warrant for refusing to disclose it. In applying the harm test, the default position or presumption is that information should be open to the public and that firm evidence is required to shift this presumption.

A simple step to apply the consequential harm test:

1. *Check the requested information. What information is precisely being request by requester;*
2. *Check which harm as set out in the Article 17 of Law 14/2008;*
3. *Check harm as set out in other law. Remember: consequential harm test only applies with law –not with any kind of regulation under the law.*
4. *Check exceptions to the exception as set out in the Article 18 of Law 14/2008;*

The fact that the information has historically been considered secret is irrelevant; the whole point of Law 14/2008 is to change the nature of secrecy in government. At the beginning of the process of implementing a right to information law, it will be difficult for officials to make good assessments of the risk of harm from disclosing information. A normal tendency, particularly in the early stages of implementation, is to push towards over-classification. PPIDs should keep this tendency in mind and think carefully about whether the harm they have identified is substantial, likely, and causally related to the disclosure before they decide to withhold information.

First, the decision-maker should advert to the relevant interest which is at risk, based on the exceptions set out in Article 17 of Law 14/2008, and the nature of the threat to that interest. Only harms which relate to the specific interests protected by Law 14/2008 should be considered. The potential for harm or embarrassment, whether to a public authority or a private person, is not a legitimate consideration, and information should never be withheld on that ground.

At this stage, the assessment should be as precise as possible. The decision-maker should advert to the nature of the harm of prejudice which is threatened. This will depend on the type of interest being protected. Thus, in relation to privacy, the key issue will be whether in fact, in relation to that individual, the information is private (thus, an email address would normally be considered private, but it would not be if it had been posted on the internet).

This stage of the process also involves an assessment of the degree of the harm that might occur. Minor harms should not be used to deny access to information; instead, the harm should be 'real', 'actual' and 'of substance'. For example, a politician might claim that he should not have to indicate what restaurant he ate in using public funds because this would reveal his 'private' food preferences. This is at best an extremely limited privacy interest which should not be allowed to defeat a request for information.

The decision-maker should also advert to whether removing or blacking out some of the information would avoid the risk of harm. In doing so, the idea is to remove the least possible amount of information that would effectively accomplish this, while also recognising that it is far better to remove some information than to deny access to the whole document.

Second, the presumption in favour of disclosure means that the risk of the harm occuring should not be specualtive or remote, but clear, concrete and plausible, as well as significant, imminent and direct. It is not enough if intervening events would be required to realise the harm.

Timeliness can also be an important consideration, since many harms are time dependent. The sensitivity of a new weapons system declines over time, criminals gradually get to know about new police investigative tactics and most innovative business approaches also become known over time. The assessment of harm should thus be based on the harm that might result from disclosure of the information at the time of the request.

Third, a causal relationship must be established between the release of the information and the risk of harm. Thus, for example, where a commercial business is doing poorly, release of certain information may indicate why it is failing. The information should normally be released despite this. Simply indicating why the business is doing poorly will not necessarily harm the business. It is only where the information would actually help the business' competitors, or harm the business directly in some way, that it may be withheld. For some more complex areas, such as law enforcement and commercial competition, a more technical assessment may be necessary.

Officials should consider only the harm which would result from disclosing the specific information being requested and not the broader category to which the information belongs. To give an example, Law 14/2008 protects law enforcement information. Most of the information that a police department holds will be connected to law enforcement, but this does not mean that police departments are wholly excluded from the law. Rather, only information which will impact negatively on law enforcement should be exempt from disclosure.

4. Public Interest Test

If a harm has been identified, the next step is to weigh the public interest. The public interest test assesses whether information which will cause harm to a protected interest should still be disclosed or withheld based on a consideration of the larger public interest.

In applying the consequential harm test, the PPID should have noted the precise nature and gravity of the harm that would likely result from disclosing the information. For the public interest test, this harm must be compared against the public interest in releasing the information.

A number of key issues should be taken into account when assessing the public interest in disclosure of the information. The impact of providing the information in terms of people's ability to participate in the decision-making process and public confidence in Indonesia's democracy are key considerations. Others include the need to maintain a proper system of public accountability and oversight, and the public interest in understanding the mechanisms of government.

The exposure of human rights violations and crimes against humanity are clearly interests of the very greatest importance, which should always, or almost always, override any secrecy interest. Other key interests include exposing corruption or breaches of the law, or risks to public health or safety or the environment. Protecting the constitution has also been recognised as an overriding public interest, as has protecting the rights of individuals against losses.

The purpose of the request may also have some bearing, though decision-makers should be careful in considering this. Everyone is equal under the law, and every Indonesian has an equal right to information. At the same time, if the PPID knows that an applicant plans to use the information for an important purpose, this can enhance the public interest in disclosure. For example, if an NGO needs certain information for environmental protection

purposes, or to measure Indonesia's progress in promoting gender equality, this may tip the scales in favour of disclosure.

Examples:

Imagine that a requester asked for personal financial information that a public body holds about a government official which revealed that the official had been embezzling money. The first step would be for the PPID to find and review the information. Having done so, they would likely discover that it engaged the exception for personal information, since release of the records would be a breach of privacy for that official. However, the degree of harm for that breach would be moderate, and not as severe as, say, releasing medical information, since the latter is generally more sensitive. By contrast, the public interest in exposing corruption is extremely high, so in this circumstance the correct decision would be to disclose the information.

Imagine that the Indonesian army carried out a deployment to East Kalimantan and, during the course of the mission, it was accused of killing people in a particular village. A requester asked for information about how the army had deployed, since that would reveal whether or not there had been soldiers in the area when the killings took place. The PPID might locate the information and conclude that its disclosure would reveal information about the Indonesian army's tactics, which would have some potential to harm the defence and security of the State if it gave away how the army might behave in future deployments. However, where an accusation of human rights abuses has been made, there is a very strong public interest in getting to the bottom of it, in order to ensure proper accountability in the government, to create a sense of public trust in the armed forces and to ensure that there is no impunity for those who carry out human rights abuses. In this case, regardless of whether or not the information revealed that the soldiers had committed the crimes, the public interest would weigh in favour of disclosure, because the matter is so serious that there is a very high need for openness and clarity.

5. The Specific Interests Which are Protected

The list of exceptions, as spelled out in Article 17 of Law 14/2008, is as follows:

1) Law enforcement
2) Intellectual property rights and preventing unfair business competition
3) The defence and security of the state
4) The natural wealth of Indonesia
5) National economic security
6) Foreign relations
7) Personal information
8) Deliberative information
9) Information that may not be disclosed under another law

1. Law Enforcement

It is important to prevent the disclosure of information whose confidentiality is vital to law enforcement, including to protect the rights of parties involved in legal cases. The scope and breadth of this exception is spelled out specifically in Article 17(a) of Law 14/2008. The Law notes that this exception is limited to the types of information listed below. In other words, in seeking to apply the law enforcement exception, the PPID should be checking to see if the information would be likely to:

1. obstruct the observation and investigation process of a criminal act;
2. reveal the identity of informants, reporters, witnesses and/or victims having knowledge of a criminal act;
3. reveal criminal intelligence data and plans related to prevention and treatment of any forms of transnational crime
4. endanger the safety and lives of law enforcement personnel and/or their families; and/or
5. endanger the security of equipments, facilities and/or infrastructures of law enforcement personnel.

The law enforcement exception applies only if one of these interests is specifically engaged. Moreover, Article 18(1) provides a list of exceptions to this exception. If information falls into one of the following categories, it cannot be exempted from disclosure:

a. verdict of court of law;
b. affirmation, decision, regulation, circular letter or other types of policies, either binding or nonbinding, internally or externally, and any consideration of law enforcement institutions;
c. warrant to discontinue investigation or prosecution;
d. annual expenditure plan of law enforcement institutions;
e. annual financial report of law enforcement institutions;
f. report of corruption fund restitutions;

Article 18(1)(g) also refers to Article 11(2), which provides for the disclosure of information that has been declared open through a process of information dispute settlement.

Other laws may also be relevant to openness in the context of law enforcement. For example, Law No. 13 of 2006 on Witnesses and Victims Protection[2] states that witnesses or victims that are under the protection of the Witness and Victim Protection Agency (LPSK) have the right to access information about developments in cases in which they are involved, as well as the right to information about when the defendants in these cases are going to be released. Thus, although the Law on Public Information Disclosure treats all citizens equally, the Law on Victim and Witness Protection, whose purpose is to protect victims and witnesses, provides them with a special right to information.

2. Intellectual Property and Unfair Competition

As part of their regular functions – whether pursuant to their regulatory role or to contracting services – public bodies collect large amounts of commercial information from private companies or individuals. It is important to safeguard sensitive private commercial

[2] Law No. 13 of 2006 on the Victim and Witness Protection, Articles 30(2) and 41.

information in order to ensure that the free market system can operate in a healthy and fair manner. Sometimes, the disclosure of information to a commercial rival would upset this balance, giving that competitor an unfair advantage. Additionally, where commercial information is given to the government voluntarily, it can be important to maintain confidentiality to ensure that private companies continue to feel comfortable handing over their information to public authorities.

Intellectual property rights generally relates to property of an intellectual or knowledge-based nature that has economic value, and that requires protection in order to ensure that the owner can exploit its economic benefits. This sort of protection is important to encourage individuals and companies to invest time and money in developing innovations, since the intellectual property framework will enable them to extract profit from them, which will benefit society as a whole.

Understanding what constitutes commercially sensitive information which should be off-limits to requesters generally involves looking for three characteristics: (1) the information is not broadly known within the relevant field of technology and/or business; (2) the information has economic value; and (3) the owner has made reasonable efforts to keep the information confidential.

3. National Defence and State Security

The interest in protecting national security requires some information to remain classified. However, Article 17(c) limits this exception to:

> Public Information that, if disclosed and provided to Public Information Requester, could endanger State defense and security, namely as follows:
>
> 1. any information concerning strategy, intelligence, operation, tactic and technique related to operation of state defense and security system, which covers the stages of planning, implementation, and finishing or evaluation in relation to domestic of foreign threats.
> 2. any document containing strategy, intelligence, operation, technique and tactics relating to the operation of state defense and security system, which cover the stages of planning, implementation, and finishing or evaluation;
> 3. any figure, composition, disposition or dislocation of strength and ability in the implementation of state defense and security system and its development plan;
> 4. any visualization and data regarding military base and/or military installation situation and condition;
> 5. any estimation data of foreign countries military and defense capacity in relation to all Actions and/or indication of such countries that may endanger the sovereignty of the Republic of Indonesia and/or data related to military cooperation with other countries that have been agreed in the agreement as confidential or very confidential;
> 6. state encoding system; and/or
> 7. state intelligence system.

In determining whether information should be exempted under this category, a key consideration may be how specific the information is. Very broad or general information will

be far less likely to facilitate harm to national interests. Similarly, older information will be less likely to cause harm than information about an ongoing campaign or deployment. It is very important to conduct a strict harm test in relation to national security so as to overcome our often unreasonable assumptions about this. Developed democracies, including the United States, disclose vast amounts of information about defence, without this in any way harming their security.

4. Natural Resources

According to Article 17(d), public bodies may withhold information which would reveal the natural wealth of Indonesia. The underlying idea here is to protect Indonesia's national sovereignty and control over its resources, rather than to hide its natural wealth as such. Indeed, being open about natural wealth can often prevent corruption or other forms of misuse of this wealth. As a result, when considering this exception, PPIDs should ask whether disclosing the information would facilitate the unauthorised exploitation of Indonesia's resources or whether opening up the information would in fact help to protect Indonesia's resources.

5. National Economic Security

This exception is to protect the national economy. The idea here is to ensure that economic policies undertaken by the Government are not compromised through untimely disclosure of information about them. For example, disclosing an interest rate change before it is made public for everyone could allow certain individuals to engage in unfair business practices so as to make money from this. Another example might be a government investigation into the health of the banking sector; premature disclosure of the investigation might lead to investors withdrawing their money from banks and thereby harming the economy.

Article 17(e) limits the information that can be withheld under this exception to seven specific categories:

1) any initial plan of sales or purchase of national or foreign currency, shares and vital assets of the state;
2) any initial plan of exchange rate adjustments, credit interest rates, and financial institution operation model.
3) any initial plan of bank credit interest rate adjustments, government loans, tax reform, tariff, or other state/local revenues;
4) any initial plan of sales or purchase of land or property;
5) any initial plan of foreign investment;
6) any process and result of supervisions concerning banks, insurance companies, or other financial institutions; and/or
7) other matters related to money printing process.

6. Foreign Relations

Relations between nations can be delicate, and governments may need to respect the secrecy of sensitive diplomatic documents in order to protect their relations with foreign powers or to ensure that the government is not disadvantaged in future negotiations.

According to Article 17(f), this category of exceptions is limited to information about:

> 1) any position, bargaining power and strategy that will be and has been by the State in relation to international negotiation;
> 2) any international diplomatic correspondence;
> 3) any communication system and encoding system used in carrying out international relations; and/or
> 4) any protection and security of Indonesian strategic infrastructure overseas.

7. Personal Information

The right to privacy is universally recognised and it is important to respect it both at a personal level in terms of fostering human development and at a political level in terms of maintaining fundamental democratic rights. In order to feel free, individuals must be able to choose their level of engagement and expression within society, and this includes privacy. Most governments hold enormous amounts of information about their citizens, much of which is sensitive. The exception for personal privacy is defined in Article 17(g) as including information that "if disclosed could reveal content of any personal authentic certificate and a person's last wish or testament."

Article 17(h) further defines personal information as:

> 1) any history and condition of family members;
> 2) any history, condition and treatment, physical and psychological medication of a person;
> 3) any financial condition, asset, income and bank account of a person;
> 4) any evaluation results concerning capability, intellectuality, and recommendation of a person's capacity; and/or
> 5) any note concerning a person's formal and non-formal education activities.

There are two cases where these exceptions do not apply, which are spelled out in Article 18(2):

> Not included as exempted information as referred to in Article 17 letter g and letter h, provided that, inter alia:
> a. the party whose secrets being disclosed grants written consent; and/or
> b. the disclosure is in relation to a person's position in public offices.

In other words, individuals to whom the information relates have the ability to consent to its disclosure. If the PPID is able to contact them, they should do so, since consent would eliminate the need to carry out further analysis, simplifying the decision-making process. Information should also be disclosed if it relates to a person's position in public office. Information relating to a person's position can be any kind of information, such as the formal description of the position, the salary range of the person or the location of the work.

It is broadly recognised that prominent public officials have a lower expectation of privacy than average citizens due to their personal importance to the State. The higher up an official

is, the less privacy they should expect, as a way of ensuring accountability. Information subject to disclosure relating to senior officials can be any kind of information, from medical records, which may be indicative of a person's mental competence to wield power, to financial records which have the potential to shed light on institutional corruption.

In many cases, blacking out or redacting individuals' names or other identifying information, especially from datasets, can avoid privacy concerns.

8. Deliberative Information

While transparency is vitally important, all governments need a certain amount of space to operate. The basic idea here is to ensure that those involved in forming government policy are comfortable speaking their mind, and to foster an environment of candour and the free and frank exchange of ideas. It is possible, for example, that a government employee might otherwise not offer an honest assessment of a co-worker's performance out of fear that their opinion might eventually be made public.

This exception is spelled out in Article 17(i):

> memorandum or letters between public bodies or within public bodies, which in nature classified, unless determined otherwise by the verdict of the Information Commission or court of law.

The Elucidation of Article 17(i) clarifies the scope of this exception by stating:

> "classified memorandum" means memorandum or letters within a Public Body or between Public Bodies which according to its nature shall not be provided to parties other than the public body carrying out correspondence activities with the respective Public Body and if opened may seriously harm policy making process, namely that may:
>
> 1. diminish freedom, courage, and honesty in submission of suggestions, communication, or exchange of ideas in relation to decision making process.
> 2. Impede the success of the policy due to premature disclosure.
> 3. obstruct the accomplishment of a negotiation process that will be or is being carried out..

In interpreting this exception, PPIDs should consider whether the release of the information would harm governmental deliberative processes. A key consideration will be whether the document reveals a policy or programme which has not been publicly announced, or over which discussions remain ongoing. Generally, it is far less likely that information will impede policymaking if it relates to a process or discussion which has been concluded, and even less likely where that policy has been announced publicly.

9. Other Information

This category refers to information classified by other legislation, namely the following laws:

Law	Classifications

Law no. 10 of 1998 regarding Banking	Reports on the results of bank examinations. Customer lists and their account information.
Law no. 5 of 1999 regarding the Prohibition of Monopolies and Unhealthy Business Competition	The identity of anyone who reports criminal activity or violations of Law no. 5/1999.
Law no. 36 of 1999 regarding Telecommunications	Information which is sent or received by a customer of a telecommunication service through a telecommunication network and/or telecommunication service.
Law no. 30 of 2000 regarding Trade Secrets	Methods of production, methods of processing, or any other technological or business information which has economic value, is not generally known and is kept secret.
Law no. 48 of 2009 regarding the Judiciary	Information regarding judicial deliberations.
Law no. 29 of 2004 regarding Medical Practice	Medical records.