# Draft Analysis of the Access to Information Bill (2016)

## January 2017

*Note: This analysis has been prepared based on the ATI Act as passed into law by the Tanzanian parliament on September 7, 2016, as available on the parliament website[1].*

*It draws heavily on expert analyses of the earlier versions of the bill, prepared by the Tanzania Freedom of Information Coalition, the Centre for Law and Democracy (CLD) in Canada, the African Freedom of Information Centre (AFIC) in Kampala, Uganda, and the Commonwealth Human Rights Initiative (CHRI) in New Dehli, India, and on Twaweza's own analyses of the same.*

---

## 1. Introduction

An Access to Information (ATI) Act was passed into law by the Tanzanian parliament on September 7th, 2016. This was amended slightly from the bill that had been presented to the Tanzanian parliament for first reading on June 23rd, 2016, and revised more substantially from a bill the government planned to bring before parliament in 2015 under a certificate of urgency but which was withdrawn following media and public pressure.

Legislation enabling public access to information was a flagship commitment of Tanzania's Open Government Partnership (OGP) Action Plan for 2014-2016. Such a law could, in principle, go a long way towards bringing the government closer to the people – allowing the public, civil society, the media and others to better understand what the government is doing, and encouraging more and better public participation in decision making processes.

Further, the Access to Information Act is an opportunity to give greater meaning to clauses in the Tanzanian Constitution, specifically Articles 18(1) and 18(2) that provide for the right to information, stating:

> *"Without prejudice to expression the laws of the land, every person has the right to freedom of opinion and expression, and to seek, receive and impart or disseminate information and ideas through any media regardless of national frontiers, and also has the right of freedom from interference with his communications."*
>
> *"Every citizen has the right to be informed at all times of various events in the country and in the world at large which are of importance to the lives and activities of the people and also of issues of importance to society."*

This note examines the ATI Act in its final, enacted version, and compares it both to the previous versions (dating from 2015 and June 2016) and to an "ideal" access to information bill. Part 2 provides a summary of the main conclusions of this analysis, while Part 3 provides a more detailed analysis.

---

[1] See http://parliament.go.tz/polis/uploads/bills/acts/1480402363-SHERIA%206-THE%20ACCESS%20TO%20INFORMATION%20ACT.pdf

## 2. Summary assessment

### Right and scope of access, and exemptions

The scope of the Act (clause 2) includes all public authorities and any private bodies that receive public funds or hold information of significant public interest. This is a wide range of organisations, presumably including government contractors, civil society organisations and even the media. It is good that the scope is defined so as to include those providing services to or for the government, but there are potential privacy and freedom of speech concerns raised by extending the scope as far as this.

The Act (in clause 5) provides right of access to information only to citizens of the United Republic of Tanzania. This excludes other residents, and appears to exclude requests made by legal entities such as corporations. In both cases, this runs contrary to global best practice.

Clause 5(2) provides one very broad exemption that could hamper implementation of the law significantly – namely by stating that information should only be provided "subject to the provisions of other written laws". Given that several other laws – such as the Records and Archives Management Act (2002) and many others – place tight controls on the release of information, this is potentially a very wide-ranging exemption.

Otherwise, the list of exemptions provided in clause 6 is reasonable for the protection of national security, personal privacy, legally privileged information, etc. It is odd that the recognised standard of access to information relating to national security – the Tshwane Principles – was not adopted, but the exemptions provided here are broadly appropriate.

Finally, in clause 18, there is a provision that makes it an offence for recipients of information under the Act to "distort" the information provided. This replaces, and significantly improves upon, previous wording that made it an offence to share or publish the information received. The term "distort" is highly subjective, however and it would have been preferable for this clause to have been removed entirely. Alternatively, it could have specified that only deliberate and malicious distortions should be an offence, or included an exemption for acting in good faith.

### Requesting procedures

In clause 10, the Act allows the use of paper or electronic communications to make requests, and includes a requirement for information holders to provide appropriate assistance to those who are illiterate or who have a disability. The same clause also requires, however, that requests must be made in a prescribed form, to be defined in subsequent Regulations, which is unnecessary and introduces an additional possible justification for refusing a request.

The final version of the bill (in clause 21) removes reference to fees being charged for making a request, allowing only that charges for "actual costs" involved in producing the requested information. This is a significant improvement on earlier versions, and brings this aspect of the law into line with international best practice. It should be applauded.

There are a number of minor concerns regarding the procedure for information holders responding to requests. First, the time limit, at 30 days, is longer than in most countries with effective ATI legislation. Second, there is no requirement to acknowledge receipt of a request. Third, there is a provision to pass a request on to a different institution that could be open to abuse.

In clause 17, the Act explains how requested information should be provided, including special consideration for those with sensory disabilities. This is largely positive, though there is also some unclear language here that it may be necessary to amend for clarity.

Finally, clause 14 clearly (and reasonably) explains how an information holder should act in the case of a refusal to provide information. However, it makes no provision to deal with situations where part of the requested information is to be refused and part should be provided.

## Appeals and sanctions

There are serious problems with the mechanisms outlined for appeals against decisions – refusals, delays, etc. – of the information holder. Most significantly, in the vast majority of possible cases, the final decision on appeals rests with the Minister with responsibility for legal affairs. This represents a clear conflict of interest, with a senior government figure given the final decision on whether information held by government should be released. It would have been preferable for appeals to be heard and judged by the courts. Further, there is no detail of where the burden of proof lies in such cases.

The Act does not establish any form of independent Information Commission. In many countries, such a commission is responsible for handing appeals, and for other important roles such as promotion and monitoring (see below) that are not assigned to anyone in this Act.

There are some strong provisions against damaging or destroying information to prevent disclosure (clause 22), and protections for whistle-blowers (clause 23) and for those acting in good faith (clause 24).

However, there is a major concern with a related issue: penalties for wrongly releasing information are severe – three to five years' imprisonment (clause 6) – while there are no penalties for wrongly withholding information. As such, from the perspective of an information holder, the risk is all on one side: wrongly release information and a long prison sentence awaits, but wrongly withhold information and there are no consequences. The effect is that the incentive built into the bill is entirely against the release of information.

## Implementation, monitoring and promotion

The Act (in clause 7) requires that all information holders should appoint an information officer, and that where this has not been done, the head of the institutions becomes the default information officer. This is a key feature of good access to information legislation and is all included here.

The Act (clauses 8 and 9) requires information holders to maintain and publish records of the information they hold. Aside from some looseness in the language used, these provisions are broadly useful.

However, there are very significant gaps in the provisions for monitoring and promotion – indeed there are no such provisions. There is no obligation on any specified body to promote the right to information or raise public awareness of the Act. There is no provision for training for information officers. And there is no requirement either for information holders or any central body to monitoring implementation of the Act. In other countries, it is usual for information holders to be required to report annually on requests received, responded to, refused, etc., and for a central body to compile an annual report on the same. Without these

provisions, it will be very difficult for anybody either within or outside government to know how well the Act is being implemented in practice, or to identify where it could be improved.

## Conclusions

There are many aspects of this Act that should be applauded. Notably, it defines information holders to include private sector bodies that receive public funds of hold information of public interest, it includes a reasonable list of exemptions focused on national security, privacy and proper legal processes, and it takes the need of those with a disability or who are illiterate into account. Moreover, some improvements were made in the final amendments, including the removal of fees for those requesting information and a change in the previous "killer clause" that made it an offence to publish or share information received under the Act.

However, four very significant weaknesses remain in place.

First, the Act allows a broad exemption in cases where another law governs the handling or release of information. In international best practice, access to information laws are given priority over other legislation in situations where the laws conflict. In the Tanzanian case, the other laws take precedence. Since there are many laws on the Tanzanian statute books that tightly control access to information, this significantly weakens the Act.

Second, the procedure for appeals against decisions of information holders includes a clear conflict of interest. In the vast majority of possible cases, the final decision on such appeals rests with the Minister responsible for legal affairs – making it very straightforward for the government to withhold any information if it wishes to do so. A better system would have been for appeals to be handled by the courts, or by an independent Information Commission.

Third, there is a major concern with the penalties for information holders who act in contravention of the Act. The penalty for wrongly releasing information is severe – three to five years' imprisonment – while there are no penalties mentioned for wrongly withholding information. The incentive for information holders is therefore very clear: by releasing information you take a big risk, it is far safer to refuse to do so.

Fourth, the lack of an independent Information Commission also means there are no provisions for promotion or monitoring of the Act. Without such provisions, particularly for monitoring, it will be very hard for anyone to assess how well the law is being implemented, to identifying good and bad practice or to identify and resolve problems.

In addition, there are numerous other concerns. While less substantial than those described here, they still represent unnecessary obstacles to effective access to information.

Taken separately, none of these weaknesses has the effect of fatally undermining the Act. There is no single killer clause. However, in combination, they represent a series of obstacles that make things difficult for those requesting information, and indeed for those in government who are minded to release information. Conversely, they make things a lot easier for those who wish to withhold information.

In its current form, the Act represents a step forward for transparency in Tanzania, but only a small one. It remains a long way short of its full potential.

# 3. Detailed analysis

## 3.1 Right and scope of access, and exemptions

### 3.1.1 Scope

Clause 2 explains which bodies the act will apply to:

> *2 (1) This Act shall apply to Mainland Tanzania.*
>
> *(2) Without prejudice to the provisions of subsection (1), this Act shall apply to:*
> *(a) public authorities;*
> *(b) private bodies registered under any written law which:*
> *(i) utilize public funds; or*
> *(ii) are in possession of information which is of significant public interest.*

This is a broad provision that the law does not just cover all government agencies, but also covers a large number of private bodies – including any that use public funding (such as contractors and suppliers of goods and services to government, subsidised industries, political parties, and more) and any that hold information of significant public interest. Potentially, this last sub-clause could include a very wide range of organisations, including civil society organisations, the media companies in extractive industries, etc.

While in some ways, this broadness of scope is good, it does raise some questions with regard to privacy and freedom of speech. Should a law of this nature really apply so broadly to private bodies?

### 3.1.2 Right of access

Clause 5 provides a clear right for Tanzania citizens to access information held by government:

> *5 (1) Every person shall have the right of access to information which is under the control of information holders.*
>
> *(2) The information holder shall, subject to the provisions of section 6 and any other written laws, make available to the public or, on request, to any person, information which is under his control.*
>
> *(3) Nothing in this Act shall limit or otherwise restrict any other legislative requirement for a public authority to disclose information.*
>
> *(4) For purposes of this section, "person" means a citizen of the United Republic*

Clause 5 (4) restricts the right of access to Tanzanian citizens only, and appears also to provide access only to natural persons, not to legal entities. In both cases, these are deviations from global best practice for access to information law.

Clause 5 (2) limits the right of access to information in two significant ways. First, section 6 of the bill provides a list of exemptions (see part 3.1.3 of this analysis). Second, this clause makes it clear that the law does not override other laws that specifically block access to information. Given the broad nature of restrictions on access to information included in other laws such as the Statistics Act (2015), The Records and

Archives Management Act (2002), National Security Act (1970) and many more, this is a very significant limitation on the new law's scope.

### 3.1.3 Exemptions

Clause 6 sub-clauses (1)-(3) lists exemptions:

> *6 (1) Notwithstanding the provision of section 5, the information holder may withhold the information where he-*
> *(a) is satisfied that all the information or part of the information is exempted under subsection (2); and*
> *(b) determines, in accordance with this Act, that the disclosure is not justified in the public interest.*
>
> *(2) Exempt information may be withheld if the disclosure of such information is likely to-*
> *(a) undermine the defence, national security and international relations of the United Republic;*
> *(b) impede due process of law or endanger safety of life of any person;*
> *(c) undermine lawful investigations being conducted by a law enforcement agent;*
> *(d) facilitate or encourage the Commission of an offence;*
> *(e) involve unwarranted invasion of the privacy of an individual, other than an applicant or a person on whose behalf an application has been made;*
> *(f) infringe lawful commercial interests, including intellectual property rights of that information holder or a third party from whom information was obtained;*
> *(g) hinder or cause substantial harm to the Government to manage the economy;*
> *(h) significantly undermine the information holder's ability to give adequate and judicious consideration to a matter of which no final decision has been taken and which remains the subject of active consideration; or*
> *(i) damage the information holder's position in any actual or contemplated legal proceedings, or infringe professional privilege;*
> *(j) undermine Cabinet records and those of its committee; or*
> *(k) distort or dramatize record or data of court proceedings before the conclusion of the case.*
>
> *(3) For purposes of paragraph (a) of subsection (2), information relating to national security includes-*
> *(a) military strategy, doctrine, capability, capacity or deployment;*
> *(b) foreign government information with implications on national security;*
> *(c) intelligence operations or activities, sources or information capabilities, methods or cryptology;*
> *(d) foreign relations or foreign activities;*
> *(e) scientific, technology or economic matters relating to national security; or*
> *(f) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to national security.*

For the most part, this is a reasonable list of exemptions. And clause 6 (1) (b) very usefully provides a public interest override that means even information on the list of exemptions should be disclosed if doing so is in the public interest.

It would have been preferable for the list of exemptions for reason of national security was based on the globally-recognised Tshwane Principles[2] for exempting national security information from freedom of information law. It is not clear why these were not followed in this case.

[2] For the Tshwane Principles, see http://www.right2info.org/exceptions-to-access/national-security/global-principles

However, the final bill represents an improvement over the 2015 version, in that the specific exemption given to the Tanzania Broadcasting Corporation (TBC) has been removed.

### 3.1.4 Use of information provided

Clause 18 introduces a restriction on the use of information provided:

> *18 (1) Subject to the provisions of section 6, a person who receives the information from the information holder shall not distort such information.*
>
> *(2) Any person who contravenes the provisions of subsection (1) commits an offence and shall, upon conviction, be liable to imprisonment for a term not less than five years.*

In an earlier version of the bill, section 18(1) stated that information received "shall not be for public use", fundamentally undermining that version. The new text allows public use of information received, and only requires that the information shall not be distorted.

This is an unusual provision that is not seen in most ATI legislation. It is not clear that it is really necessary. Further, lack of clarity in the term "distort" means the clause remains problematic. It is a highly subjective term. One person may consider something to be a natural and honest interpretation of information provided, while another may consider the same interpretation to be a distortion.

To reduce the possibility of misinterpretations, it would have been preferable to specify either that only "deliberate and malicious" distortions should be considered to be an offence, or introduce an exemption for acting in good faith. Better still would have been to remove section 18 in its entirety.

## 3.2 Requesting procedures

### 3.2.1 Making requests for information

Clause 10 provides the procedure for requests:

> *10.-(1) A request for access to information shall be made in a prescribed form and addressed to the information holder.*
>
> *(2) The request for information shall provide sufficient details to enable the information holder to identify the information and shall include name and address of the person requesting the information.*
>
> *(3) For purposes of subsection (1), a request shall be treated as made in writing where the text of the request*
> *(a) is delivered by hand, postal, or transmitted by electronic means;*
> *(b) is received in legible form in the manner prescribed in the regulations; and*
> *(c) is capable of being used for subsequent reference.*
>
> *(4) A person requesting who, because of illiteracy or disability is unable to make a written application for access to information, may make a request orally, and the officer to whom the request is made shall reduce the request into writing in the prescribed form and provide a copy of the written request to the person requesting.*

There are some strong points within this clause. In particular, it provides for requesters to use paper or electronic means of communication, and it has a specific provision requiring information holders to assist those who are illiterate or disabled to make their request.

A minor complaint is that the final version of the Act requires that requests be made using a prescribed form (to be laid out in regulations at a later date). This may help in simplifying the process of responding to requests, but it also provides an additional possible justification for refusing a request.

### 3.2.2 Fees and costs

Clause 21 provides for fees:

> *21. The information holder from which a request for access to information has been made may charge fees necessary for covering actual costs for production of the requested information.*

This represents an improvement on earlier versions of the bill, which had specified that fees would also be charged for the act of making a request. This has been removed, leaving only fees to cover "actual costs" for production of requested information. As a result, this aspect of the law is now in line with international best practice for freedom of information law: that no fees should be charged for requests, but that information requests can be asked to cover specific actual costs involved with responding to requests – such as photocopying costs.

### 3.2.3 Responding to requests

Clauses 11, 13 and 16 outline the key procedures to be followed by information holders in dealing with requests, including the time allowed for responses:

> *11 (1) Where access to information is requested, the information holder to which the request is made shall, as soon as practicable but not exceeding thirty days after the request is received-*
> *(a) give written notice to the person who made the request as to whether the information exists and, if it does, whether access to the information or a part thereof shall be given; and*
> *(b) if access is to be given, promptly give the person requesting access to the information or a part thereof in the manner prescribed under this Act.*
>
> *(2) Where the information holder requires further information in order to identify and locate the information requested, it shall, within fourteen days of receiving the request for information, notify the person requesting of the need for such further information and in that case, the period of fourteen days shall be reckoned from the date on which such further information is received.*
>
> *(3) Where the information holder is satisfied that the information requested*
> *(a) does not exist; or*
> *(b) has already been published and it is in public domain,*
> *the information holder shall inform the person who made the request to that effect.*
>
> *13 (1) Where the information holder to which a request for information is made considers that another information holder is the appropriate holder of the information requested, the information holder to which the*

*request was initially made may, as soon as practicable but not exceeding seven days after the request is received, transfer the request to such other information holder and give a written notice of the transfer to the person who made the request.*

*(2) For the purpose of subsection (1), the period specified in section 11 shall apply to the information holder to which the request is transferred with effect from the date on which the request is transferred.*

There are several minor concerns here that could usefully have been addressed.

First, 30 days (clause 11 (1)) is longer than is provided in many access to information laws. A 20-day limit, or even 14 days, is more common.

Second, there is no requirement for information holders to acknowledge that a request has been received. This potentially introduces confusion as to whether a request has been received, and when the 30 day (or shorter) time limit applies.

Third, the provision to transfer a request to a different organisation (clause 13) is unusual and problematic. By allowing an information holder to transfer a request merely because they "consider" that another body is "the appropriate holder of the information requested", the bill provides a very easy means for information holder to avoid providing information. Potentially, this could create a lengthy or unending process of institutions passing on requests to each other without the requester ever being provided with the information.

### 3.2.4 Means of providing requested information

Clause 17 explains how information should be provided to those who requested it:

*17.-(1) Access to information may be provided to a person in any of the following forms:*
*(a) provision of a copy of the information;*
*(b) delivery of a copy of the information in electronic form;*
*(c) in the case of an information that is an article or another thing from which sounds of visual images are capable of being reproduced, by making arrangements for the person to hear or view sounds or visual images;*
*(d) in the case of an information by which words are recorded in a manner in which they are capable of being reproduced in the form of sound of in which words are contained in shorthand writing or codified, by provision of a written transcript of the words recorded or contained in the information;*
*(e) in the case of a person with a sensory disability, by provision of a record in a format that allows the person to read or listen to the record of the information.*

*(2) Where a person who made the request has requested access in a particular form, the information holder may issue the information in a form he deems proper.*

*(3) Where the form of access requested:*
*(a) contravenes the provisions of the National Security Act;*
*(b) interferes unreasonably with the operations of the information holder;*
*(c) is detrimental to the preservation of the information or having regard to the physical nature of the information it is not appropriate;*
*(d) would involve inordinate huge cost or time to the information holder; or*
*(e) would involve an infringement of copyright other than a copyright owned by the government subsisting in the information, access in that form may be refused and given in another form.*

There are some strong points here, notably including special consideration for those with a sensory disability. However, there is some strange or ambiguous language that may require amendments at some point – sub-clauses (2) and (3) for example would appear to be poorly arranged, and it is not clear what "an information" may be.

### 3.2.5 Refusals

Clause 14 explains the procedure for refusals by information holders to provide information:

> *14.-(1) Where the information holder refuses to give access to information requested, either in whole or in part, such information holder shall, in writing, notify the person requesting the information of the refusal and shall, in the notification:*
> *(a) set out reasons for the refusal and all material issues relating to the decision, including the specific provision of this Act and the factors taken into consideration in relation to the public interest;*
> *(b) inform the person who made the request of the availability of a review in accordance with section 19 within which an application for review may be made;*
> *(c) where the decision is to the effect that the information does not exist, state that a thorough and diligent search was made to locate the information.*

This clause has several good provisions – for notifications and reasons for refusals, information regarding appeals, and a statement that delayed responses constitute refusal.

However, the bill does not in this or any other clause state what should be done in circumstances where some part of the requested information is exempt and some is not – a "severability" clause.

## 3.3 Appeals and sanctions

### 3.3.1 Appeals

Clause 19 outlines the procedure for appeals, in cases where a request has been denied.

> *19.-(1) A person who, having made a request for information, is aggrieved by a decision of the information holder in relation to the request, may apply to the head of institution for review of the decision in respect of any of the following:*
> *(a) refusal of access by the information holder to the information requested;*
> *(b) payment of fees or charges which the person considers unreasonable;*
> *(c) failure of the information holder to comply with time limits set out under this Act;*
> *(d) any other matter relating to a request for or access to information made under this Act.*
>
> *(2) The head of institution shall, within thirty days of receiving an application made under subsection (1), determine such application for review in accordance with its own laid down procedures.*
>
> *(3) Any party aggrieved by the decision of the head of institution made under subsection (2) may, within thirty days from the date of receiving such decision, appeal to the Minister whose decision shall be final.*
>
> *(4) Notwithstanding subsection (3), where the requested information is within the authority of an information holder who is under the Minister, the Minister shall cease to be the appellate body and any aggrieved person may apply to the High Court for review.*

This route for appeals – first to the head of institution, second to the Minister (of Legal Affairs) "whose decision shall be final", no further appeal – has some problems. Most significantly, giving the final decision to the Minister represents a conflict of interest, where a senior representative of government has the final say on whether information is released. A small set of cases – where an information holder is under that particular Minister – the appeal can be redirected to the High Court. This is a new provision included only in the final version of the Act, presumably to reduce conflicts of interest, but it achieves this goal only in a very narrowly defined set of circumstances.

It would be preferable for the second appeal to be handled by judicial review (as in the 2015 version) or by the courts. Alternatively, a third appeal against the Minister's decision could be included for all cases, with this third appeal handled by judicial review.

Further, despite repeated calls to do so, the Act does not establish a specific Information Commission. In many countries, this is the institution that handles appeals (along with other responsibilities for monitoring implementation of the bill, requiring public bodies to change their information management systems, etc.). The lack of such an institution leaves the bill weak in several areas (see also section 3.4.3 of this analysis).

Finally, there is no detail on where the burden of proof lies in the appeals process. Under the best access to information laws, the government is required to demonstrate that it did not operate in breach of the rules.

### 3.3.2 Sanctions for information holders

Clauses 6 (6) and 22-24 provide for sanctions against information holders who do not adhere to the law:

> *6 (6) Any person who-*
> *(a) disclose exempt information, other than information relating to national security, commits an offence and shall, on conviction be liable to imprisonment for a term not less than three years but not exceeding five years.*
> *(b) discloses exempt information relating to national security, commits offence and the provisions of the National Security Act shall apply.*

> *22. A person who alters, defaces, blocks, erases, destroys or conceals any information held by the information holder, with the intention of preventing the disclosure by such information holder, commits an offence and shall, on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding twelve months or to both.*

> *23 (1) A person in the service or employment of any information holder shall not be subject to any legal, administrative or employment related sanctions for releasing information on wrongdoing, or information which would disclose a serious threat to health, safety or the environment, as long as that person acted in good faith and in the reasonable belief that the information was substantially true.*
>
> *(2) For purposes of subsection (1), wrongdoing includes the commission of a criminal offence, failure to comply with a legal obligation, a miscarriage of justice, corruption or dishonesty, or maladministration regarding the information holder.*

*24. Officers in the service or employment of any information holder shall not be subject to any civil or criminal liability for any act done or omitted to be done in good faith in the exercise or performance of any power or duty under this Act*

There are some strong and clear provisions here. In particular, clause 22 against damaging or destroying information in order to prevent disclosure is strong. Further, the provisions in clause 23 to protect whistle-blowers and clause 24 to limit liability for those acting in good faith are excellent.

However, there are two significant problems.

First, clause 6 (6) represents a major threat to employees of information holders against disclosure of information. The penalty here – three to five years' imprisonment – is very severe.

Second, nowhere in the bill has it been made an offence simply to refuse to provide information. This is contrary to best practice and the AU Model FOI Law, which recommend that refusal to provide requested information should be an offence. This could easily be added to clause 22.

The contrast here – harsh penalties for wrongly releasing information and no penalty for wrongly withholding information – is stark. From the perspective of an information holder, the risk is all on one side: wrongly release information and a long prison sentence awaits, but wrongly withhold information and there are no consequences. As such the incentive built into the bill is entirely against the release of information.

## 3.4 Implementation, monitoring and promotion

### 3.4.1 Information officers

Clause 7 requires that all information holders should appoint an information officer:

*7 (1) Every information holder shall appoint one or more officers as information officers.*

*(2) An information officer shall deal with requests for information and render assistance to a person seeking such information.*

*(3) Where an information holder fails to appoint an information officer, the head of such institution shall be the information officer for the purpose of this Act.*

This is a clearly expressed requirement, and a key element in effective implementation of access to information laws.

### 3.4.2 Public records of information

Clauses 8 and 9 (1) and (2) require that information holders should maintain records of information held, and to make key details of information held available to the public:

*8 (1) Every information holder shall maintain record of information that are under the control of such information holder.*

*(2) For the purpose of subsection (1), the information holder shall maintain every record for a period of not less than thirty years after a date on which the information is generated or a date on which such information came under the control of the information holder.*

*9 (1) Every information holder shall, not later than thirty six months after the commencement of this Act, issue a notice to the public in the Gazette, website or news paper of wide circulation, containing the following:*
*(a) a description of its structure, functions, and responsibilities including those of any of its statutory officers or advisory committees;*
*(b) statutory officers or advisory committees; and*
*(c) a general description of categories of information held by such information holder.*

*(2) the notice shall include particulars of the officer to whom requests for official information or particular classes of information shall be sent.*

A small change was made to clause 8 in the final wording, compared to the 2015 version. The previous version included the word "complete" – i.e. "complete records of information" – which has now been dropped. It is unclear why this change has been made, and the completeness of records is important.

It is also a little concerning that the Act gives such a long period of time for information holders to issue their notices regarding the information they hold.

### 3.4.3 Promotion and monitoring

There are significant gaps in the provisions for promotion and monitoring. First, there is no general obligation on any specific body (such as an Information Commission) to promote the right to information, and no requirement for public awareness raising. Second, there is no provision for training for information officers or other employees of information holders.

Third, the bill has no requirement for monitoring implementation. In international best practice, it is usual to require information holders to report annually to a central body (such as an Information Commission), and to require that central body to report annually to parliament. Alternatively, reports could be submitted directly to parliament. In either scenario, reports should include information on the number of requests for information received, responded to positively, refused and appeals.

Without any such provisions, it will be much harder both for government and others to track implementation of the Act – to identify institutions that are performing better or worse than expected, or to identify significant blockages in the system.