



MEMORANDUM

TO

MINISTER IN THE PRIME MINISTER'S

DEPARTMENT

(LAW AND INSTITUTIONAL REFORM)

YB DATO' SRI

AZALINA OTHMAN SAID

23 JANUARY 2024

**MEMORANDUM
TO
MINISTER IN THE PRIME MINISTER'S DEPARTMENT
(LAW AND INSTITUTIONAL REFORM)
YB DATO' SRI AZALINA OTHMAN SAID
23 JANUARY 2024**

Issued by:

Centre for Independent Journalism (CIJ)
Center to Combat Corruption and Cronyism (C4)
Sinar Project
ARTICLE 19

Endorsed by:

Suara Rakyat Malaysia (SUARAM)
KRYSS Network
Gerakan Media Merdeka (Geramm)
Sisters in Islam (SIS)
Justice for Sisters
Freedom Film Network (FFN)

**MEMORANDUM
TO
MINISTER IN THE PRIME MINISTER’S DEPARTMENT
(LAW AND INSTITUTIONAL REFORM)
YB DATO’ SRI AZALINA OTHMAN SAID
23 JANUARY 2024**

Contents

EXECUTIVE SUMMARY	1
INTRODUCTION.....	2
PARAMETERS	2
ALIGNMENT OF LAWS.....	7
Official Secrets Act 1972	7
Section 203A of the Penal Code.....	12
Personal Data Protection Act (PDPA) 2010	13
Whistleblower Protection Act 2010	16
RECOMMENDATION	18
ANNEX 1 International RTI Principles that inform CSO Model Bill.....	i
ANNEX 2 RTI Rating Table for select countries.....	ii

EXECUTIVE SUMMARY

1. Right to Information (RTI) is internationally recognised as a human right as enshrined in Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR). It is also intrinsic to Article 10 of the Federal Constitution. A viable right to information regime requires three elements:
 - a. Substantive legal right to information and a framework for its exercise and protection. This encapsulates the basic rationale that access to official information is a basic right;
 - b. Those legal rights must be supported with amendments to legal provisions governing official secrets, heavy sanctions for 'unauthorised' disclosure, protection of data privacy held by public authorities and protection for disclosure in good faith and for public interest; and
 - c. Reforms must be impactful to replace the existing culture of secrecy with one of openness and transparency.
2. Any restrictions to disclosure and access to public information must be grounded upon international human rights standards of legality, necessity and proportionality. Exceptions should be limited and narrowly defined and always assessed on a case-by-case basis. A harm test needs to be applied to justify non-disclosure, and there should be exceptions to non-disclosure where public interest overrides the harm to the protected interests.
3. Proactive disclosures and ease of access to information are integral parts of a progressive information regime. Mechanisms to institutionalise proactive disclosure and information request processes need to be supported by an efficient, reliable and accountable data management system for data collection, management, use, storage and disposal of data.
4. In order to ensure effective implementation of the law, an oversight body in the form of a RTI commission should be established. This body should be politically independent and receive the necessary financial and human resources to carry out its functions. The oversight body should have the power to receive appeals to refusals to disclose information, order the disclosure of information and issue administrative functions to public bodies that fail to comply with the RTI law.

INTRODUCTION

1. The core RTI coalition comprising the Centre for Independent Journalism (CIJ), Center to Combat Corruption and Cronyism (C4), Sinar Project and ARTICLE 19 lauds the Minister's reply in Parliament that the Legal Affairs Division, in the Prime Minister's Department (Bahagian Hal Ehwal Undang-undang- BHEUU) is in the process of identifying parameters, and challenges in implementation that includes aligning laws that contradict the spirit of information freedom¹ following the Prime Minister's announcement of enacting a Freedom of Information (FOI) law at the federal level and amending the Official Secrets Act 1972 (OSA)² to ensure effective alignment at the Special Cabinet Committee on National Governance. A progressive right to information regime will promote a culture of transparency and contribute to enhancing the public's trust in the governance process.

PARAMETERS

2. Malaysia can soon join Indonesia, Thailand, Vietnam and Philippines as countries in ASEAN with legislation on RTI or Freedom of Information (FOI), as well as 129 other countries worldwide. It would be useful to draw from good practices and learn from the experiences of other countries in the drafting of the RTI Bill, as well as in developing effective mechanisms and structures of implementation towards building an enabling environment for the public's right to access information in Malaysia.
3. A RTI legislation has two primary functions:
 - a. Sets a clear framework on how information held by public bodies is managed and proactively disclosed to the public, and setting the exhaustive and limited grounds for restriction of certain disclosures; and
 - b. Establishes a mechanism and service standards for the public to request access to public information. This creates an obligation for public bodies to receive and respond to requests in a timely manner, mandates the allocation of organisational human resources, and creates an appeal process where a formal, fair and independent process can be initiated to review the refusal of information requests.³
4. The principles on RTI legislation were originally developed in 1999 and updated in 2015. They have been endorsed by Abid Hussain, the UN Special Rapporteur on Freedom of Opinion and Expression, in his report to the 2000 Session of the United

¹ "Legal Affairs Division identifying parameters, challenges to enact Freedom of Information Act – Azalina", New Straits Times, 9 Nov 2023, <https://www.nst.com.my/news/nation/2023/11/976598/legal-affairs-division-identifying-parameters-challenges-enact-freedom>

² "Govt agrees to enact Freedom of Information Act", Malaysiakini, 14 Sep 2023, <https://www.malaysiakini.com/news/679282>

³ Centre for Independent Journalism, A Preliminary Assessment of the Early Years of State FOIE Implementation in Malaysia, Oct 2021 (revised Feb 2022), page 1

Nations Commission on Human Rights (E/CN.4/2000/63), and referred to by the Commission in its 2000 Resolution on freedom of expression, as well as by Hussain's successor Frank LaRue in 2013 in his report to the UN General Assembly in 2013 (A/68/362, 4 September 2013). The nine principles are: **Maximum disclosure; Obligation to publish; Promotion of open government; Limited scope of exceptions; Processes to facilitate access; Costs; Open meetings; Disclosure takes precedence and Protection for whistleblowers.**

5. In institutionalising the right to information, supported by a culture of transparency and openness, it would be meaningful for Malaysia to be guided by the following set of principles and standards that would promote and protect our right to information, including through the enactment of a RTI legislation.

a. Maximum Disclosure/ Open by default

i. RTI works on the fundamental premise that all information held by governments and public institutions are in principle public, and may only be withheld or not disclosed if there are legitimate grounds recognised under international law, such as national security, privacy, law enforcement, commercial and other confidentiality, public or individual safety, and the effectiveness and integrity of government decision-making processes.

ii. Disclosure of information should not be dependent on the goodwill of the government when they feel certain information should be released or restricted but follow the principle of maximum disclosure whereby all information held by public bodies should be in principle subject to disclosure. The public also has a right to receive information, and so, they should be able to access data and information in a timely and easily accessible manner. The principle of maximum disclosure establishes a presumption that all information held by public bodies should be subject to disclosure and that this presumption may be overcome only in very limited circumstances. The overriding goal of legislation should be to implement maximum disclosure in practice.

b. Obligation to publish

i. The mandate of proactive disclosure means that request for information is only necessary when information is not publicly available. The Government should proactively publish all information on the relevant sites and ensure that it is routinely updated and easily accessible. This would allow the public to access the information in a timely manner.⁴

ii. Proactive transparency needs to be supported by good infrastructure that is user friendly, including an up-to-date database or data

⁴ Cited in Helen Darbishire (2009) "Proactive Transparency: The future of the right to information? A review of standards, challenges and opportunities", World Bank, page 34, https://foiadvocates.net/wp-content/uploads/Publication_WBI_ProactiveTransp.pdf

inventory, as well as regular conduct of data audits to uphold the highest standards of information accessibility and integrity.

- iii. Monitoring compliance with proactive disclosure obligations by public bodies is necessary to ensure transparency. Low compliance of proactive disclosure occurs where there is a lack of an accountability mechanism, legal mandate or an absence of sanction. In the UK, monitoring exercises by the Information Commission led to the shift from voluntary proactive disclosure to mandatory disclosure. Indicators issued by Information Commissioners in Mexico, resulted in an increase in proactive disclosure compliance.

Minimum standards of proactive disclosure and progressive implementation of proactive transparency

It has been established that proactive disclosure could be “user-driven”, where governments take note of the trends of demand from frequent RTI requests, and publish such information to save time for both officials and potential information requestors.

c. Independent, administrative oversight body

The government should not be the gatekeepers of information who have the final say on what the public should know and how the public can get the information. There should be an independent body set up to ensure that appropriate processes and procedures are in place to guarantee access to information relevant to public interest - with sufficient safeguards to its autonomy and ability to function without political interference.

d. Promotion of open government

Civil service should be trained on the culture of delivering information to the public, not preventing them from obtaining it. The culture of openness can be developed progressively. ARTICLE 19 points to the culture of openness evident in countries with a long history of access to information, where disclosure of information is a norm, whilst “withholding information is considered unusual”⁵. In Sweden, access to public records is seen as a “self-evident civil right”⁶.

e. Exceptions to disclosure

- i. Some information can be withheld and not disclosed, such as private data and information which may threaten national security. There should be legitimate, necessary and proportionate grounds for not disclosing information. The list of exceptions must be clearly articulated in the legislation and must not be too broad and open to arbitrary interpretation. Information that is withheld should be routinely reviewed to ensure that the exemption still applies.

⁵ “Asia Disclosed: A Review of the Right to Information across Asia”, 2016, ARTICLE 19

⁶ “Asia Disclosed: A Review of the Right to Information across Asia”, 2016, ARTICLE 19

- ii. A harm test must be carried out to protect the public's interest before restricting or denying access to information in line with international standards of the 3-part test of legality, necessity and proportionality (legitimate aim to non-disclosure, harm to the legitimate aim, harm outweighs public interest).
- f. Cost
- i. The cost of gaining access to information held by public bodies should not prevent people from demanding information of public interest, given that the whole rationale behind right to information laws is to promote open access to information. The public should not be required to pay any fee to request for data or information held by public authorities. Fees should only exist to cover the costs of material reproduction such as photocopying and printing.
 - ii. Good practices include: it is free in India where requests are made orally by persons without internet access⁷ and by persons living below the poverty line⁸. As taxpayers' money is used to generate publicly held information, the Information Commission in Slovenia mandates that there should be no cost for information that is for public interest.⁹
- g. Open meetings
- The public should be able to know about the government's plans. For example, before a forest reserve is being considered for degazettement, there should be mandatory open hearings/ consultations for the public's input - where details and information of the planned projects are fully disclosed to the public. Meetings should be open where input from potentially impacted members of the public is sufficiently taken into account, whether it is about macro national issues such as education or local issues such as advertising billboards, as these are decisions that affect the public.
- h. Reviewing other legislation
- There is a need to ensure that implementation of a RTI law will not be impeded by existing laws. There must be a complete review or amendment of laws or legal provisions which impede RTI.
- The oversight information commission in France is given a mandate beyond the FOI law (Commission on Access to Administrative Document) as a measure to mitigate the situation where proactive disclosure provisions are spread across a number of laws.¹⁰

⁷ Helen Darbshire (2009) "Proactive Transparency: The future of the right to information? A review of standards, challenges and opportunities", World Bank, page 29 https://foiadvocates.net/wp-content/uploads/Publication_WBI_ProactiveTransp.pdf

⁸ Centre for Independent Journalism (CIJ), Comparative Study: Structures and Status of Implementation of RTI Legislations (Afghanistan, India, Indonesia, Sri Lanka, Australia, United Kingdom) (2021), page 13

⁹ Helen Darbshire (2009) page 29

¹⁰ Helen Darbshire (2009) page 35

i. Protecting whistleblowers

Whistleblowers should be protected to the fullest extent. If an information officer exposes corruption, that officer should be rewarded, not punished and provided with avenues to protect themselves from harm.

j. Promotion of the law

The RTI law should include a provision placing a duty upon the Information Commission to inform the public of their right to information through promotion of a culture of openness. Promotional activities should include at list public awareness campaigns to the general public. The public education should focus on the dissemination of information regarding the right to access information. To this end, the Information commission should develop a school curriculum about the right to information and how to exercise it.

The law should also include a requirement that public bodies provide comprehensive right to information training for their officers.

k. RTI law to be reviewed regularly

Regular reviews by the Information Commission and Parliament would be able to ensure that the people are really benefiting from the legal recognition of the right to information. The RTI Commission should publish annual reports assessing the implementation of the law by public bodies.

6. In developing the new federal RTI Bill, the government can refer to a recommended legislative text for a federal RTI legislation (*to be shared later*) and parameters of the CSO Model Bill on RTI (*to be shared later*) developed by civil society groups after undergoing extensive consultations since civil society led the national campaign for a Freedom of Information Act in 2006.

7. In addition, the global RTI rating¹¹ by the Centre for Law and Democracy (CLD) which examines the strength of the national legal framework for accessing information held by public authorities may serve as a useful reference for the government in drafting the substantive elements of the federal RTI law. If Malaysia's upcoming federal RTI legislation is able to meet minimum international standards, it should be able to receive a respectable RTI rating and score reasonably well against seven categories of indicators¹² representing key elements of a right to information system: (a) Right of Access, (b) Scope, (c) Requesting Procedures, (d) Exceptions and Refusals, (e) Appeals, (f) Sanctions and Protections, and (g) Promotional Measures.¹³

¹¹ Global Right to Information Rating: The RTI Rating analyses the quality of the world's access to information laws. Global Right to Information Rating Map <https://www.rti-rating.org/>

¹² Centre for Law and Democracy (CLD) and Access-Info, Note on the Application of the RTI Rating Methodology, <http://www.law-democracy.org/wp-content/uploads/2011/09/COVER-NOTE.pdf>

¹³ For more information, refer to

Annex 1 for International RTI Principles that inform CSO Model Bill on RTI

Annex 2 for RTI Rating Table for select countries

ALIGNMENT OF LAWS

Official Secrets Act 1972

The culture of secrecy that is embedded and institutionalised under the OSA is incompatible with RTI that is grounded on the principles of transparency and openness.

8. Issues with OSA

a. Broad Executive Power to Classify and Immunity from Scrutiny

Minimal safeguards against broad Executive powers where judicial discretion can be applied to review classification was essentially removed by the 1986 amendments to the OSA.¹⁴ The additions of section 2B and 16A meant that the Executive is given broad legal discretionary powers on classification. Further, both these provisions do not require the inclusion of substantive justification in the classification of information, thus raising the issue of accountability.¹⁵

- Section 2B empowers public authorities who are accountable to the federal (Minister) and state (Chief Minister) legislatures, as well as “any public officer” appointed by the Minister or Chief Minister to classify information as “top secret”, “secret”, “confidential” or “restricted”.
- Section 16A states that exercise of the power of classification under section 2B cannot be challenged in court. Even though the different categories of classification of documents by public authorities recognised under section 2B is guided by broad definitions¹⁶ found in regulations under “*Arahan Keselamatan*”¹⁷, such guidelines do not override section 16A.¹⁸

¹⁴ Centre for Independent Journalism, Recommendation Paper Aligning OSA and other restrictive laws to a new RTI law (2021), page 3, <https://cijmalaysia.net/aligning-official-secrets-act-osa-1972-with-a-new-federal-rti-legislation/>

¹⁵ ibid page 4

¹⁶ Broad definitions of categories of “official secret” located found in publicly available slides presented by CGSO representative <https://www.slideshare.net/lszwanShah/arahan-keselamatan-34846329>

Rahsia Besar: Dokumen, maklumat dan bahan rasmi jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia

Rahsia: Dokumen, maklumat dan bahan rasmi jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.

Sulit: Dokumen, maklumat dan bahan rasmi, jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan Malaysia atau kegiatan Kerajaan atau individu atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau menguntungkan kuasa asing.

Terhad: Dokumen, maklumat dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakan juga diberi satu tahap perlindungan keselamatan.

¹⁷ Center to Combat Corruption and Cronyism, Position Paper on the Official Secrets Act: Repeal, Review or Stay? Moving from Secrecy to Open Governance (2016), page 6 <https://c4center.org/position-paper-official-secrets-act/>

¹⁸ Centre for Independent Journalism, Recommendation Paper Aligning OSA and other restrictive laws to a new RTI law (2021), page 4

b. Classification by Category removes accountability by public officials

The Schedule of “Official Secrets” is in conflict with Right to Information because classification by category removes accountability by public officials to determine or interpret whether a piece of information is an ‘official secret’, given that information is deemed as an ‘official secret’ if it falls under the categories in the Schedule.¹⁹

i. The Schedule provides the following categories of documents that are presumed as official secrets and need not be issued with a certificate of classification as stipulated under section 2B:

- Cabinet documents, records of decisions and deliberations including those of Cabinet committees.
- State Executive Council documents, records of decisions and deliberations including those of State Executive Council committees.
- Documents concerning national security, defence and international relations.

ii. Further, the Minister of Home Affairs is empowered under section 2A to add, amend or delete provisions in the Schedule through gazetted orders and the Schedule may be also amended through legislative process via Parliament.²⁰

c. Classification by levels of security is broad, not clearly defined and not subject to harm/ public interest test

Aside from legitimate limitations to disclosure e.g. where it harms national security, defence, or foreign relations, the “*Arahan Keselamatan*” also allows permissible classification such as information that embarrasses the government of the day as being ‘confidential’.²¹

Further, the absence of a harm test to justify secrecy or lack of application of public interest test as an exception to disclosure on classified information²² is in conflict with the international standards of the 3-part test (legitimate aim to non-disclosure, harm to the legitimate aim, harm outweighs public interest) for justifying non-disclosure.

¹⁹ Centre for Independent Journalism, Recommendation Paper Aligning OSA and other restrictive laws to a new RTI law (2021), page 6

²⁰ *ibid* pages 5-6

²¹ Center to Combat Corruption and Cronyism, *Position Paper on the Official Secrets Act: Repeal, Review or Stay? Moving from Secrecy to Governance* (2016), page 10

²² *ibid* page 10

d. Criminalisation of primary and secondary disclosures of classified information

The broad range of offences under the OSA where any person in possession of 'official secret' information is presumed to have intent to disclose or act against national security interest, has the burden of proof to prove otherwise, and is subject to heavy penal sanction,²³ is problematic.

- i. **Obligation to report:** Any person which includes a public servant or private parties with contractual ties with the government has the obligation to report requests for 'official secret' information to their public authority superior or enforcement agency (Section 7A), and failure to report will subject the person to imprisonment of one year minimum upon conviction (Section 7B).²⁴
- ii. **Possession of an 'official secret' without authority:** Any person who holds an 'official secret' document is presumed to have the intent to use it to the detriment of national security. The burden of proof is reversed and lies with the accused to prove that they have no intent of using the document 'for any purpose prejudicial to the safety of Malaysia'. Further, penal consequences are heavy with a minimum imprisonment of one year (Section 9(2)).²⁵
- iii. **External parties associated with a person in possession of 'official secret':** Section 12 and Section 28 places responsibility upon and penalises external parties who are not directly involved in the possession or disclosure of 'official secret'.
 1. Telecommunication companies are required to hand over messages used to communicate classified information, and failure to comply will result in imprisonment of one year minimum upon conviction (Section 16).²⁶
 2. Where an offender is a company, corporation, member of a partnership or firm, Section 28 places the same legal liability for the offence on every director, officer or member of company, corporation or partnership unless they can prove no knowledge or consent and have taken measures to prevent such an offence.²⁷

²³ Center to Combat Corruption and Cronyism, *Position Paper on the Official Secrets Act: Repeal, Review or Stay? Moving from Secrecy to Governance* (2016), page 10

²⁴ *ibid*, pages 7-8

²⁵ *ibid*, page 8

²⁶ *ibid*, page 8

²⁷ *ibid*, pages 8-9

9. Proposed reform of OSA²⁸

Significant and meaningful reform of the OSA needs to take place in tandem with the federal RTI legislation to prevent the possibility of conflicts between disclosure obligations and retention of a secrecy regime undermining the right to information in principle and practice.²⁹

a. Enactment of the federal RTI law and reform to the OSA should be harmonised.

b. Limit the breadth of Executive's power on classification:

- i. Amend Section 2 which defines the term "official secret" with reference to the Schedule: Delete "any document specified in the Schedule and any information and material relating thereto and" after "'official secret' means"

"official secret" ~~means any document specified in the Schedule and any information and material relating thereto and~~ includes any other official document, information and material as may be classified as "Top Secret", "Secret", "Confidential" or "Restricted", as the case may be, by a Minister, the Menteri Besar or Chief Minister of a State or such public officer appointed under section 2B; "photographic apparatus" means any apparatus for taking or making of photographs, film, negative, tape or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom and includes any component part of such apparatus; "police officer" includes any person upon whom the powers of a police officer not below the rank of Inspector are conferred by the Minister under section 29;"

- ii. Delete Sections 2A and 2B that confers power to the Minister to amend the Schedule and for public officials to be appointed to classify official documents;
- iii. Delete Schedule which contains the list of classes of information that are presumptively "official secrets";
- iv. Delete section 16A which immunises the exercise of the power under section 2B from judicial scrutiny.

²⁸ For more information on reform to OSA, refer to

- i. CIJ's Recommendation Paper Aligning OSA and other restrictive laws to a new RTI law (2021)
- ii. C4's Position Paper on the Official Secrets Act: Repeal, Review or Stay? Moving from Secrecy to Open Governance (2016)

²⁹ Centre for Independent Journalism, Recommendation Paper Aligning OSA and other restrictive laws to a new RTI law (2021), page 7

- c. Introduce a new provision to include power to classify a subject to specified legitimate aims and a harm/public interest test

Amend section 2B which empowers elected federal and state legislative representatives and public authorities to classify information to apply the following 3-part test for classified information: (1) a recognised legitimate aim; (2) harm to the legitimate aim if information were disclosed; (3) public interest in not disclosing the information outweighs the public interest in disclosing it.³⁰

Amend, but substituting the text with the following:

“(1). A Minister, the Menteri Besar or the Chief Minister of a State may ~~appoint any public officer~~ by a certificate under his hand to classify any official document, information or material as "Top Secret", "Secret", "Confidential" or "Restricted", as the case may be.

(2) Information may only be classified under subsection 1 if:

- *(a) its classification would be justified by an aim specified in subsection 3;*
- *(b) its non-classification would cause serious harm to the relevant aim; and*
- *(c) the public interest classifying the information outweighs the public interest in the information not being classified.*

(3) For the purpose of this section, the legitimate aims which may justify the classification of an information are:

- *(a) the protection of national security; and*
- *(b) the protection of public or individual safety.*

(4) A certificate for the classification of a document, information, or material under subsection 1 must:

- *(a) specify the legitimate aim for the exemption;*
- *(b) state the anticipated serious harm to the legitimate aim that will be caused if the document, information, or material is not classified; and*

³⁰ Centre for Independent Journalism, Recommendation Paper Aligning OSA and other restrictive laws to a new RTI law (2021), page 8

- (c) declare that such serious harm would outweigh the public interest in the non-classification of the document, information, or material.”³¹

d. Introduce a new provision for right to appeal against decisions to classify

Add a new section under OSA

Certificates issued under section 2B are subject to appeal under Right to Information Act.

e. Insert a statutory defence of public interest into OSA where any impugned act that was made under a reasonable belief in public interest, the person shall not be held liable.³²

Section 203A of the Penal Code

10. Issues with Section 203A of the Penal Code related to RTI³³

Section 203A(1) of the Penal Code prohibits disclosure of any information obtained in the performance of an individual’s duties or functions under any written law. As such, this section largely pertains to the performance of a public official’s duties. Section 203A(2) extends criminal liability to any persons who obtained such information knowing that such information was obtained during performance of a legal duty or function. The maximum punishment imposed is a fine not more than RM1 million, or imprisonment not more than 1 year, or both.

The existence of a penal sanction upon the very act of disclosing any sort of information within the conduct of public service functions contributes towards a culture of secrecy within the public service, where whistleblowing is deemed antithetical to the ethos of the office.

The inherent uncertainty surrounding the legitimate aim of s. 203A creates major barriers to legal protection afforded under WPA 2010, rendering its application unnecessarily complicated for both whistleblowers and enforcement officials. This is evident from the fact that there are no successful prosecutions under s. 203A since its enactment, casting serious doubts regarding its impact and utility.

³¹ Centre for Independent Journalism, Recommendation Paper Aligning OSA and other restrictive laws to a new RTI law (2021), page 8

³² *ibid* page 16

³³ The following are passages from C4 Commentary 01/24: A Decade of Section 203A and its Impact on Whistleblowers (Unpublished) by Lee Poh Hong and Arief Hamizan.

11. Proposed Reform of Section 203A of the Penal Code

As part of the Right to Information Act, to facilitate whistleblowing a new subsection needs to be inserted on statutory defence of public interest disclosure, so that any person who is believed to have ‘reasonably’ made public interest disclosures should be exempt from any punitive sanctions.³⁴

Since it is questionable whether s. 203A has added any positive value to anti-corruption commitments and efforts against organised crimes, the most prudent course of action is to completely repeal s. 203A.

Several compelling justifications support the removal of s. 203A. Firstly, its negligible usage by law enforcement agencies renders it practically redundant. Secondly, repealing s. 203A would introduce much-needed clarity in the practical application of WPA 2010. In particular, the complete repeal of s. 203A would ultimately resolve the apparent conflict between s. 203A and s. 6 WPA 2010, thus enhancing whistleblower protection to civil servants and enforcement officials.

Finally, the removal of s. 203A would foster a culture of open accountability in the Malaysian society and facilitate the recognition of every Malaysian’s freedom of information, which is an integral part of the enshrined freedom of expression. This move would empower grassroots capacity building initiatives in educating the public and enhancing awareness of corruption issues. Ultimately, it would garner collective support vital for the government’s anti-corruption initiatives.

Personal Data Protection Act (PDPA) 2010

12. Issues with PDPA related to RTI

- a. Limited application of the Act
 - i. The Act does not apply to federal government and state governments (section 3). This means that the Act as governed by 7 principles (section 5(1) that include disclosure, security, retention of data, data integrity principles) does not impose any limitations on how the federal and state public sectors collect, store and use personal data.
 1. Even though the government is the largest holder of personal data of its citizens, the public sector cannot be held accountable for any privacy violations under this Act.
 2. Further the public sector does not need to adhere to the exception to the disclosure principle where disclosure of personal data is allowed under circumstances such as public interest (section 39).

³⁴ Centre for Independent Journalism, Recommendation Paper Aligning OSA and other restrictive laws to a new RTI law (2021), page 16

- ii. The scope is limited to commercial transactions only and does not apply to credit reporting agencies. This limitation also excludes data collected by educational institutions, religious or non-profit organisations.

- b. Absence of mandatory notification of data breach under duty of data users (section 33): Data breaches severely undermine Malaysia’s ambition for a complete digital transformation, if there are no commensurate penalties or recourse.
 - i. In 2023, the CIJ monitoring recorded six significant instances of data breaches. The Penang government's official website experienced a breach, with over 600,000 rows of private data allegedly stolen and uploaded to BreachForums³⁵. Universiti Teknologi Mara (UiTM) faced scrutiny for a data leakage incident involving nearly 12,000 applicants' information. Prudential Malaysia confirmed a cybersecurity attack on its subsidiaries due to a MOVEit zero-day vulnerability exploit³⁶. The Credit Counselling and Debt Management Agency (AKPK) acknowledged a data breach, anticipating further data publication on the dark web³⁷. Concerns arose regarding potential data leaks from the Inland Revenue Board (LHDN) website³⁸.
 - ii. The mid-year threat landscape report of 2023 released by CyberSecurity Malaysia³⁹, revealed that the government sector in Malaysia faced the highest number of data breaches, accounting for 22% of all breaches at 46 instances of data breaches, while the telecommunications sector led in the volume of data leaked at 424.92GB.

- c. The office of the Commissioner lacks independence and has limited powers: The Minister has vast powers in relation to the powers of the Commission; dismissal, remuneration and oversight of the office.

³⁵ *Penang government data leaked online | Free Malaysia Today (FMT)*. (n.d.). Retrieved November 28, 2023, from <https://www.freemalaysiatoday.com/category/nation/2023/02/09/penang-government-data-leaked-online/>

³⁶ *UiTM apologises for data leak involving 12,000 varsity applicants | The Star*. (n.d.). Retrieved November 28, 2023, from <https://www.thestar.com.my/news/nation/2023/05/10/uitm-apologises-for-data-leak-involving-12000-varsity-applicants>

³⁷ Reporters, F. M. T. (2023, April 26). *Data from IT breach published on dark web, says AKPK*. Free Malaysia Today (FMT). <https://www.freemalaysiatoday.com/category/nation/2023/04/26/data-from-it-breach-published-on-dark-web-says-akpk/>

³⁸ Reporters, F. M. T. (2023, March 1). *Taxpayers’ data secure, LHDN says after alleged leak*. Free Malaysia Today (FMT). <https://www.freemalaysiatoday.com/category/nation/2023/03/01/taxpayers-data-secure-lhdn-says-after-alleged-leak/>

³⁹ *“CyberSecurity Malaysia report: Government sectors suffered most data breaches, while telcos spilled over 400GB of data in H1 2023”*, The Star, 25 Oct 2023 <https://www.thestar.com.my/tech/tech-news/2023/10/25/cybersecurity-malaysia-report-government-sectors-suffered-most-data-breaches-while-telcos-spilled-over-400gb-of-data-in-h1-2023>

- i. The Minister is entitled to exercise the power to direct the Commissioner, who is responsible directly to the Minister (section 59), which may compromise the independence of the Commissioner in fulfilling their mandate;
- ii. The Minister may at any time revoke the appointment of the Commissioner (section 54), and has the power to determine remuneration and allowances of Commissioner (section 57), which compromises the independence of the Commission due to the lack of security;
- iii. No requirement for the Commission's annual reports to be subject to Parliamentary scrutiny or made public, as it is only required to be furnished to the Minister (section 60) further raises concern about the independence of the Commission.

13. Proposed Reform of PDPA

- a. To delete section 3(1) where the federal government and state governments are exempt from this Act.
- b. Expedite amendments to the PDPA to introduce a duty of mandatory data breach incident notification to the Commissioner within 72 hours.⁴⁰
- c. Strengthen independence of the Commissioner by making the office directly responsible to Parliament, instead of the Minister:
 - i. The Commissioner should be required to furnish their annual reports to Parliament instead of the Minister, and the reports should be tabled and debated;
 - ii. Matters such as appointment and remuneration should be placed under parliamentary vote, either by a full sitting of the Dewan Rakyat or a newly constituted Select Committee tasked with key appointments; and
 - iii. Revocation of appointment should also be placed under parliamentary vote, with exhaustive statutorily stipulated grounds for removal.

⁴⁰ Dr Muhammad Sufyan Basri, Senior Principal Assistant Director, Monitoring Division of the Personal Data Protection Commissioner Office Malaysia, Presentation at Session 2: Strengthening Digital Rights in Malaysia, International Day for Universal Access to Information (IDUAI) Forum, 5 Dec 2023, page 17

14. Issues with WPA 2010 related to RTI⁴¹

- a. **According to Section 6(1) WPA 2010**, protection is not accorded if disclosure is prohibited by any written law. For example, a person who discloses classified information under OSA with the intention of exposing improper conduct as stipulated under WPA 2010 will not be protected under this Act.
- b. Section 6(1) also stipulates that protection is limited only to those who disclose improper conduct to “enforcement agencies”, thereby excluding disclosures to internal reporting channels or media from protection.
- c. Protection must be revoked if any of the circumstances enumerated under Section 11 are believed to have emerged, with no discretion to opt against this and no centralised oversight body to evaluate the merits of the case. The enumerated circumstances include:
 - i. Section 11(1)(a): If the person has participated in the impugned act of improper conduct
 - ii. Section 11(1)(d): Disclosure principally involves questioning the merits of policy of government/public body
 - iii. Section 11(1)(f): If the whistleblower commits an offence under this Act in the course of making the disclosure or providing further information thereto.

15. Proposed Reform of WPA⁴²

- a. The proviso to section 6(1) WPA 2010 should be removed since section 11 WPA 2010 specifically deals with the exhaustive circumstances in which legal protection to whistle-blowers should be revoked. This proviso is unnecessary, confusing, vague, and difficult for enforcement agencies and potential whistleblowers to understand.
- b. A notwithstanding clause should be inserted into the WPA 2010. This clause would expressly stipulate that, notwithstanding the generality of any written laws prohibiting disclosure of any information, if the application of such laws conflict with the protective provisions under the WPA 2010 in any extent or manner, the provisions under the WPA 2010 shall unequivocally prevail.

⁴¹ For further information, see Fadiyah Nadwa Fikri, Gaps in the Act: A Legal Analysis of Malaysia’s Current Whistleblower Protection Laws (Center to Combat Corruption and Cronyism, 2021).

⁴² The following are passages from C4 Commentary 01/24: A Decade of Section 203A and its Impact on Whistleblowers (Unpublished) by Lee Poh Hong and Arief Hamizan.

- c. Statutory defences should be introduced into section 11 WPA 2010 which deals with the revocation of whistleblower protection. Particularly, these defences must consist the following cardinal features: (1) the restriction of disclosure or revocation must relate to a specific legitimate interest, (2) the disclosure of information would result in actual or threatened harm to that legitimate interest i.e. the risk of harm must be compelling, (3) the prejudicial effect of the disclosure or revocation must far outweigh the public interest considerations involved, (4) the test must be objective, (5) the burden of proof lies on the enforcement agency to justify why disclosure should be prohibited and/or whistleblower protection should be revoked, and (6) it is for the judiciary or competent tribunal to decide whether the prohibition and/or restriction is actually justified in light of legality, proportionality and necessity. For instance, such public interest defences can be manifested in the form of defence of lawful authority, reason, excuse, or justification for the disclosure of information, or in circumstances where the information disclosed is already available to the public.

- d. A list of statutory illustrations should be introduced into the WPA 2010. The illustrations to be inserted should seek to categorise certain matters presumed to be in the public interest and generally should be disclosed or afforded legal protection. These matters may include corruption-related crimes, organised crimes, money-laundering, domestic or international human rights violations, environmental harm, public safety, and abuses of public office.

RECOMMENDATION

16. We urge the State to undertake the following actions to ensure a progressive RTI regime:

- a. Set up a Steering Committee, that comprises civil society and other experts, to facilitate the drafting of the RTI bill and the amendments to the OSA. We hope the government, through the Legal Affairs Division (BHEUU) under the Prime Minister's Department, continues its engagement with multi-stakeholders in guaranteeing a progressive and substantive new legislation;
- b. Commit to a clear timeline for the alignment of OSA and other federal and state laws with the RTI federal legislation;
- c. Guarantee that the RTI federal legislation adheres to international standards
 - i. Commit to making critical adjustments to institutional structures to support the operationalisation of the law, and guaranteeing an information system that is well-resourced, progressive, promoted, monitored and enforced, in order to protect and promote the right to information.
 - ii. For proactive disclosure and open government data policy to work, commit to making all government data open by default and put in place structural mechanisms to ensure good data management policy and framework to fully optimise the potential value of government data, whilst protecting data privacy and security, and incorporate a monitoring, evaluation and enforcement mechanism to ensure realisation of the commitment to making access to information a public right.

ANNEX 1 International RTI Principles that inform CSO Model Bill

International framework with RTI Principles:

- [Article 19](#),
- the [UN Special Rapporteur on Freedom of Opinion and Expression on principles for RTI in 2000](#),
- [Organisation of American States](#).
- [African Commission on Human and People’s Rights – Declaration of Principles on FOE in Africa](#)
- [RTI-ratings on FOI/ RTI law according to the Centre for Law and Democracy \(CLD\)](#)

For specific principles regarding national security and RTI, please refer to:

- [Overview of the Global Principles on National Security and Right to Information](#) – 15 things the Principles Say
- [The Global Principles on National Security and the Right to Information \(Tshwane Principles\), 2013](#) – 50 Principles

	ARTICLE 19	Organisatio n of American States (OAS)	UNSR FOOE	Declaration of Principles on FOE in Africa	CLD Ratings on FOI/ RTI law
	2013	2005	2000	2002	
Maximum Disclosure - obligation to disclose and - public has right to receive info held by public bodies	√	√	√	√	√
Obligation to Publish- Proactive Disclosure	√	√	√	√	
Limited scope of exceptions ● Refusal with legitimate reason and written communication ● Access is the rule, secrecy the exception ● Public interest takes precedence over secrecy	√	√	√	√	√
Structures, processes, (procedures) to facilitate Access - Requests procedure should be simple, speedy - Duty to assist requestors - Strict time limit for processing requests	√	√	√		√
Cost - minimal	√	√	√		√
Disclosure takes precedence - Alignment of other laws to RTI - Secrecy laws should be amended	√		√	√	
Protection from sanction for disclosure in good faith	√		√	√	√
Promotion of open government - Open, accessible internal systems	√				√
Right to Appeal – guaranteed by an independent body	√	√		√	√
Open Meetings - Presumption of meetings of public authorities are open	√		√		√
Promotional Measures - Public education about law			√		√

ANNEX 2 RTI Rating Table for select countries

Country	RTI Ranking	RTI Rating (score out of 150)	Category of Indicators ⁴³							Date	Country
			Right of Access	Scope	Requesting Procedure	Exceptions and Refusals	Appeals	Sanctions & Protections	Promotional Measures		
Afghanistan	1	139	5	30	28	30	26	6	14	2014	Afghanistan
Mexico	2	136	6	30	28	28	26	4	14	2002	Mexico
Sri Lanka	4	131	5	28	26	23	29	4	16	2016	Sri Lanka
India	8	127	4	25	25	26	29	5	13	2005	India
Indonesia	41	100	5	28	13	16	25	3	10	2008	Indonesia
UK	43	99	2	25	19	13	23	7	10	2000	UK
New Zealand	52	94	4	16	22	18	23	6	5	1982	New Zealand
Canada	53	93	5	14	20	13	26	6	9	1983	
Australia	64	87	2	11	22	15	23	4	10	1982	Australia
Philippines	133	46	5	13	17	4	4	1	2	2016	Philippines
Max Score	138 countries	150	6	30	30	30	30	8	16		

Note: RTI Rating examines strength of national legal framework for accessing information held by public authorities. Refer to Methodology for the scoring- <https://www.rti-rating.org/methodology/>

⁴³ <https://www.rti-rating.org/country-data/by-indicator/>