Draft – ~~22~~ ~~July~~ 5 September 2022

Malawi Communications Regulatory Authority

Guidelines on Personal Data Breach Notifications and Communications

The Authority issues this document as a source of information and guide to data controllers and processors and interested parties of the general public. For this reason it should not be relied on as legal advice or regarded as substitute for legal advice in individual cases. The information contained in this document may be subjected to changes from time to time.

Table of Contents

DEFINITIONS

In these Guidelines, unless the context otherwise requires, terms have meanings assigned in the [Data Protection Act, 2022] and—

"Act" means the [Data Protection Act, 2022]; and

"engaging entity" means a data controller or data processor that engages a data processor to process personal data on its behalf or at its direction.

1. INTRODUCTION

1.1. Background

The Malawi Communications Regulatory Authority (referred to herein as the Authority) is mandated by the Act to promote the protection of personal data, regulate the processing of personal data throughout Malawi and oversee the implementation of and be responsible for the Act.

Section 33 of the Act requires every data processor to notify its engaging entity when a personal data breach has occurred. It further requires every data controller to determine whether it is required to notify the Authority and make a communication to affected data subjects when a personal data breach has occurred.

Section 33(6) of the Act requires the Authority to issue guidance on the steps to be taken by a data controller to adequately inform data subjects of a personal data breach. These Guidelines provide such guidance as well as guidance on all personal data breach notifications and communications required by Section 33 of the Act.

1.2. Purpose and application of the Guidelines

The purpose of these Guidelines is to give practical advice and guidance to data controllers and data processors when determining for purposes of Section 33 of the Act:

- whether a personal data breach has occurred;
- whether a personal data breach notification or communication is required to be made;
- the format and contents of any such required personal data breach notification or communication; and
- the deadline by which a required personal data breach notification or communication must be made; and
- the extent of records regarding a personal data breach to be kept.

These Guidelines are not a substitute for the Act or any regulations or rules issued thereunder and only serve to reflect the Authority's approach in determining compliance with the requirements of Section 33 of the Act. These Guidelines may be revised from time to time in light of new legislation, regulations, rules, legal precedent or best practices.

2. Personal data breaches

2.1. What is a personal data breach?

A "personal data breach" is defined in Section 2 of the Act as:

> *a breach of security of a data controller or data processor leading to or reasonably likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

A personal data breach requires a "breach of security," but not all breaches of security are personal data breaches.

First, the breach must involve personal data that is being processed by the data controller (or a data processor on its behalf) or data processor. If no such personal data is involved in the breach, then the breach is not a personal data breach under the Act and Section 33 of the Act would not apply.

Second, if such personal data is involved, the breach must lead to or be reasonably likely to lead to "the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to" the personal data. These terms can be interpreted using their plain meaning:

- "destruction" of personal data means the personal data either no longer exists or is no longer in a form that is usable by the data controller or data processor;
- "loss" of personal data means the personal data may still exist, but the data controller or data processor has lost possession or control of the personal data, or access to it;
- "alteration" means that the personal data has been altered, damaged or corrupted or is no longer complete; and
- "unauthorised disclosure of or access to" personal data means disclosure of personal data to, or access by, recipients who are not authorised to receive or access the data.

A personal data breach can involve one or any combination of these circumstances.

Personal data breaches are often thought of as exclusively the result of malicious actions by an external third party against an information system, such as through malware. While this is often the case, it is not the only type of breach. As the definition indicates, personal data breaches may be accidental. For example, an employee may, as a result of human error, accidently destroy or improperly disclose personal data. Also, an employee's lost smartphone or laptop lacking proper password protection may contain a trove of personal data processed by the employer. Paper-based personal data may be physically mailed to an incorrect address. Human error need not be involved in the accidental nature. For example, a natural disaster may result in damage to information systems and temporary or permanent loss of personal data. Personal data breaches may also result from deficiencies in physical security, rather than cybersecurity, allowing unauthorized access to information systems as well as paper-based filing systems.

2.2. Appropriate measures required to prevent and detect personal data breaches

Section 31(1) of the Act requires data controllers and data processors to:

> *implement appropriate technical and organizational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control, including protections against accidental or unlawful destruction, loss, misuse or alteration, unauthorized disclosure or access. . .*

These measures, including those expressly set out in Section 31(2) of the Act, are meant, among other things, to minimize the likelihood of a personal data breach. The occurrence of a personal data breach resulting from a lack of appropriate technical and organizational measures may be evidence of a violation of Section 31 of the Act.

In addition, to be considered "appropriate," such technical and organizational measures must also include an appropriate capability to detect any reasonably anticipated personal data breaches. Thus, if a data controller or a data processor experiences a personal data breach that is not promptly detected, this may also be evidence of a violation of Section 31 of the Act.[1]

Any such assessments of the appropriateness of technical and organizational measures will always take into account the following factors set out in 31(1) of the Act:

(a) the amount and sensitivity of the personal data;

(b) the degree and likelihood of harm to data subjects that could result from the loss, disclosure or other misuse of the personal data;

(c) the extent of the processing;

(d) the period of data retention; and

(e) the cost of any technologies, tools or other measures to be implemented relative to the size of the data controller or data processor.

2.3. When does a data controller or data processor become aware of a personal data breach?

The deadlines for notification of personal data breaches in Section 33(1) and (2) of the Act (see discussions of deadlines in section 3) are triggered by the data controller or data processor having become aware of the personal data breach. This standard of awareness presupposes that the data controller or data processor has implemented the appropriate technical and organizational measures required by Section 31(1) of the Act and therefore has an appropriate capability to detect any reasonably anticipated personal data breaches. Thus, any failure to become, or delay in becoming, aware of a personal data breach may be evidence of a violation of Section 31(1) (see discussion in section 2.1).

The precise moment when a data controller or data processor becomes aware of a personal data breach is fact-specific and depends on the circumstances of each breach. Often it may be immediately clear that a security breach has occurred that constitutes a personal data breach. However, this will not always be the case. A data controller or data processor may suspect a security breach but require further investigation to confirm that one has occurred. A data controller or data processor may confirm that a security breach has occurred but require further investigation to determine whether it will lead or is reasonably likely to lead to the actions that would constitute a personal data breach under the definition.

For purposes of determining awareness, the Authority will consider a data controller or data processor to be aware of a personal data breach when it has a reasonable degree of certainty that a security breach has occurred and that the breach would be likely to result in the "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." Implicit in this standard is an obligation to promptly and adequately investigate any suspected or known

[1] In addition, if applicable, a personal data breach, as well as the failure to detect it, may also be evidence of a failure to conduct an adequate data protection impact assessment, and thus may be evidence of a violation of Section 24 of the Act.

suspected breach to make this determination. Any failure to execute or delays in executing such an investigation may also be evidence of a violation of Section 31(1) (see discussion in section 2.1).

A data controller or data processor that is an engaging entity is deemed to have awareness of the breach upon receipt of a breach notification by the data processor it engaged. However, the engaging entity could reach awareness earlier. For example, it may have already reached the "reasonable degree of certainty" standard described above through other means, such as evidence within its own information systems, communications with the data processor it engaged, media reports or customer complaints. In some cases, an engaging entity could even become aware of a personal data breach affecting a data processor it has engaged before that data processor is aware of it or even suspects it.

3. Required personal data breach notifications and communications

Section 33 of the Act sets out three distinct types of personal data breach notifications and communications:

- data processor notifications to its engaging entity (Section 33(1));
- data controller notifications to the Authority (Section 33(2)); and
- data controller communications to affected data subjects (Section 33(3)).

In this section, we discuss each of these and the circumstances and timing under which such a notification is required.

Even if a notification or communication is not required by the Act, a data controller or data processor is always still free to make one. The requirements of the Act should generally be considered a floor, not a ceiling, on best practices relating to data security and data protection.

Also, a data controller or data processor may be bound by contractual or other reporting obligations beyond the scope of the Act. For example, a data processor may be contractually bound to notify its engaging entity of security breaches even if the breaches do not rise to the level of personal data breaches. A data controller may be bound by a customer agreement to report any personal data breaches to the data subject even if they are not required to make a communication to affected data subjects under the Act. A data controller or data processor may also have related regulatory notification or reporting obligations specific to its sector or business that are outside the scope of the Act.

3.1. Data processor notifications and obligations to respond to requests

A. Data processor notifications

Under Section 33(1) of the Act:

- a data processor is ALWAYS required to notify its engaging entity when a personal data breach has occurred, and such obligation is NEVER contingent upon a risk assessment; and
- the notification must ALWAYS be made within 72 hours after the data processor becomes aware of the personal data breach (see discussion in Section 2.3).

If a data processor is processing personal data on behalf of multiple engaging entities, or on behalf of one or more engaging entities and itself (making it also simultaneously a data controller), the requirement to notify an engaging entity is only triggered if the personal data breach relates to personal data processed as part of the engagement. The Act does not obligate a data processor to notify an engaging entity if the personal data processed on the engaging entity's behalf is not the subject of a personal data breach.

Even if a data processor learns of the personal data breach from its engaging entity (as discussed in section 2.3), it is still required to notify the engaging entity under Section 31(1). The data processor may have additional information about the breach that is not available to the engaging entity and would be useful in helping the engaging entity satisfy its own obligations under Section 33.

B. Content of data processor notifications

While there is no prescribed format for a data processor notification to its engaging entity, based on the requirements of Sections 33(1)(a) and 33(4) of the Act, the following information should be conveyed:

- a description of the nature of the personal data breach, including, where possible:
  - the categories of data subjects and personal data records concerned; and
  - the approximate numbers of data subjects and data records concerned;
- the name, contact details and a point of contact of the data processor;
- the likely consequences of the personal data breach (to the extent ascertainable by the data processor); and
- a description of measures taken or proposed to be taken by the data processor to address the breach, including measures to mitigate its possible adverse effects on the affected data subjects.

C. Deadline for a data processor notification

As set out above, a data processor must make the notification to its engaging entity within 72 hours after the data processor becomes aware of the personal data breach (see discussion in Section 2.3).

D. Data processor obligations to respond to information requests

Section 33(1)(b) of the Act requires a data processor to respond "without undue delay" to all information requests of the engaging entity relating to the personal data breach to allow the engaging entity to comply with its own obligations under Section 33 of the Act. The Authority interprets the phrase "without undue delay" to mean as soon as reasonably possible.

Where the personal data breach notification to the engaging entity is the first time the engaging entity becomes aware of or even suspects a personal data breach, any such information requests would be made after the notification. However, the obligation of the data processor to respond to information requests is not limited to the period after the notification. An engaging entity may become aware of or suspect a personal data breach prior to the data processor making a notification. An engaging entity's information requests

relating to a personal data breach or suspected data breach would be within the scope of Section 33(1)(b) of the Act even the request is made prior to receiving the notification from the data processor.

More generally, Section 25 of the Act requires an engaging entity to take reasonable measures to ensure that the data processor it has engaged "implements appropriate technical and organisational measures to ensure the confidentiality of personal information as required in Part V [of the Act]." Inherent in these measures is the establishment of appropriate communication channels between the engaging entity and the data processor to address matters relating to the security of personal data. The required responses to information requests required under Section 33(1)(b) of the Act should be seen as only one example of these necessary communications channels.

3.2. Data controller notifications to the Authority

Under Section 33(2) of the Act:

- a data controller is SOMETIMES required to notify the Authority when a personal data breach has occurred, depending on the outcome of a risk assessment; and
- the notification USUALLY must be made within 72 hours after the data controller becomes aware of the personal data breach (see discussion in Section 2.3).

A. Under what circumstances is a notification to the Authority required?

Section 33(2) of the Act requires a data controller to make a notification to the Authority when a personal data breach has occurred with respect to personal data processed by the data controller or a data processor acting on its behalf only when the breach is "likely to result in a risk to the rights and freedoms of individuals." To determine whether such a risk is likely to result, the data controller must conduct and document a risk assessment. If the risk assessment confirms the likelihood, then a notification to the Authority is required. If it does not, no notification to the Authority is required.

In interpreting Section 33(2), the Authority considers the term "rights and freedom of individuals" to refer solely to the rights and freedoms of the data subjects whose personal data is the subject of the personal data breach. Thus, when conducting a risk assessment, the data controller need not be concerned with the risks to the rights and freedoms of other individuals that may be affected by the breach.

Expectation that a notification is required

The Authority advises that any risk assessment start with the expectation that every personal data breach is "likely to result in a risk to the rights and freedom of individuals." However, specific, demonstrable factors may show that the breach is not likely to result in such a risk. These factors will likely be specific to the circumstances of the personal data breach and the personal data involved. Reliance on any such factors will need to be justified and documented. But we present the following guiding principles here:

- in the case of "destruction," "loss" or "alteration" of personal data, a breach is unlikely to result in such a risk if all of the destroyed, lost or altered personal data can quickly be recovered from backup copies or other sources by the data

controller or data processor, and it is unlikely that any affected data subject would be affected by the temporary unavailability;

- in the case of "unauthorised disclosure of or access to" personal data, a breach is unlikely to result in such a risk if all of the disclosed or accessed personal data is:
    - already publicly available; or
    - encrypted, de-identified, tokenized, or similarly protected using state of the art technology (assessed at the time of the breach) to make it inaccessible or unintelligible and any decryption key, mechanism for re-identification, password or similar decoding mechanism has not been compromised.[2]

B. Content of notifications to the Authority

Based on the requirements of Sections 33(1)(a) and 33(4) of the Act, the following information should be conveyed in a notification to the Authority:

- a description of the nature of the personal data breach, including, where possible:
    - the categories of data subjects and personal data records concerned;
    - the approximate numbers of data subjects and data records concerned;
- the name, contact details and a point of contact of the data controller;
- the likely consequences of the personal data breach;
- a description of measures taken or proposed to be taken by the data controller to address the breach, including measures to mitigate its possible adverse effects on the affected data subjects.

In addition, a data controller must indicate whether it intends to make a communication to the affected data subjects or a public communication, as required in some circumstances by Section 33(3) of the Act (see discussion in Section 3.3). If the data controller does not believe the personal data breach is likely to result in a high risk to the rights and freedoms of the affected data subjects and does not intend to make such communications, it should set out the rationale for such determination. If the data controller believes that the personal data breach is likely to result in a high risk to the rights and freedoms of the affected data subjects but intends to only make a public communication, it should set out the reasons why direct communications to the affected data subjects would involve disproportionate effort or expense or would be otherwise not feasible. If available at that time, the data controller should include with the notification the text of any such intended communications.

A data controller must submit the information above through any electronic submission system provided by the Authority, or in the absence of which by email to an address that the Authority shall publish on its website. The data controller must certify that the information

---

[2] When relying on this last principle, a data controller would have an ongoing obligation to monitor whether such decryption key, mechanism for re-identification, password or similar decoding mechanism remains uncompromised, or the encryption of similar technology relied upon remains effective. If the decryption key, mechanism for re-identification, password or similar decoding mechanism is later compromised or the technology is no longer considered effective, a notification to the Authority would be required at that time.

provided in the notification is true and complete. If the data controller is not a natural person, the Secretary or another officer must make the required certification on its behalf.

C. Deadline for a notification to the Authority

Section 33(2) of the Act requires a data controller to make its notification within 72 hours after becoming aware of the personal data breach (see discussion in section 2.3). However, Section 33(5) of the Act allows a data controller to extend this deadline in two limited circumstances:

- "to accommodate the legitimate needs of law enforcement"; or
- "as reasonably necessary to implement measures required to determine the scope of the breach."

In both circumstances, the data controller must "provide[ ] to the Authority the grounds for such extension, including supporting evidence" as described below.

Accommodating the legitimate needs of law enforcement

A data controller may delay submitting a required notification to the Authority if law enforcement officials have expressly requested, in writing, that the notification be delayed in order to maintain confidentiality during an investigation or accommodate other needs of law enforcement. The written request from law enforcement must detail the specific needs requiring accommodation.

In the case of such a delay, the data controller must when or before making the data breach notification:

- inform the Authority that the data controller is relying on the extension of the deadline permitted by Section 33(5) of the Act;
- explain that law enforcement has requested that a full notification not be made at that time; and
- attach a copy of the written request of law enforcement.

Implementing measures to determine the scope of the breach

A data controller may delay submitting a required notification to the Authority if it requires additional time to ascertain the scope and other details of the breach to either:

- determine whether a notification to the Authority is required under Section 33(2) of the Act; or
- allow the data controller to ascertain the information required to make a full personal breach notification.

In the case of such a delay, the data controller must submit an extension notification to the Authority which:

- acknowledges that a personal data breach has occurred;
- states that the data controller is relying on the extension of the deadline permitted by Section 33(5) of the Act;

- sets out the rationale for the delay and the steps the data controller expects to take to determine whether a full notification is required or ascertain the information required in a full notification (as applicable);
- if the delay is predicated on allowing the data controller to ascertain the information required to make a full personal breach notification, includes any partial information then available; and
- provides an estimate of when such steps are expected to be completed.

A data controller must submit this extension notification to the Authority within the 72 hours after it has become aware of the personal data breach through any electronic submission system provided by the Authority, or in the absence of which by email to an address that the Authority will publish on its website. The Authority will inform the data controller if the Authority deems the extension notification deficient, requires additional information, rejects the basis for the extension and/or requires the notification to be made by a specified date.

If a data controller submits an extension notification because it required additional time to determine whether a notification to the Authority is required under Section 33(2) of the Act, and subsequently determines that a notification is not required, it must promptly notify the Authority of such determination.

3.3. Data controller communications to affected data subjects

Under Section 33(3) of the Act:

- a data controller is SOMETIMES required to make a communication to affected data subjects when a personal data breach has occurred, contingent upon the outcome of a risk assessment; and
- the communication must be made “with undue delay;” and
- SOMETIMES a public communication in the media may replace a required communication to an affected data subject.

A. Under what circumstances is a communication to an affected data subject required?

Section 33(3)(a) requires a data controller to make a communication to a data subject if a personal data breach is “likely to result in a high risk to the rights and freedoms” of the data subject.

As with Section 33(2) of the Act (see discussion in section 3.2(A) above), the Authority considers the term “rights and freedoms of a data subject” to refer solely to the rights and freedom of a data subject whose personal data is the subject of the personal data breach.

In addition, this risk assessment may lead to the conclusion that a communication is required to be made to only some of the affected data subjects where only those are subject to the “high risk” to their rights and freedoms. This may reflect the specific personal data, attributes, circumstances and vulnerabilities relating to the data subjects.

Factors to be considered under Section 33(8) of the Act

The data controller should consider both the severity of the impact of a personal breach on the rights and freedoms of data subjects and the likelihood of these occurring. Section 33(8)

of the Act sets out three factors that a data controller may take into account when determining whether a communication is required to be made to affected data subjects.

The first factor is:

> *the likely effectiveness of any technical and administrative measures implemented to mitigate the likely harm resulting from the personal data breach, including any encryption or de-identification of the data;*

This factor will largely also be considered when assessing whether a notification to the Authority is required (see discussion in section 3.2(A)). Here, when considering the necessity of notifying data subjects about the breach, the emphasis is on the harms that the data subject may suffer, and the effectiveness of mitigating technical and administrative measures implemented. Typically, if such measures substantially mitigate the likely harm to data subjects under Section 33(8) so that it is not necessary to notify data subjects, the risk to data subjects may be low enough that no notification to the Authority is required under Section 33(2).

The second factor is:

> *any subsequent measures taken by the data controller to mitigate such risk;*

While the first factor refers to measures in place before the personal data breach, this second factor refers to any actions that a data controller, or data processor acting on its behalf, may have taken subsequent to the breach to mitigate the risk of harm to affected data subjects.

For example, in the case of “destruction,” “loss” or “alteration,” the data controller may have subsequently been able to recover the personal data and made a determination that during the time it was unavailable it is unlikely that any affected data subject could have suffered any harm. In the case of “unauthorised disclosure of or access to” personal data, the data controller may have been able to identify all individuals to whom it was disclosed or by whom it was accessed, assessed that such disclosures or access would not result in any harm to the data subjects affected and taken measures to prevent any further unauthorized disclosure or access. Or the data controller may have instituted mitigating measures, such as requiring password changes that significantly lower the risk of unauthorised access to accounts.

The third factor is:

> *the nature, scope and sensitivity of the personal data involved.*

We begin with “nature” and “sensitivity,” viewing sensitivity as one aspect of the personal data’s nature. The nature of the personal data involved in the breach is directly related to the risk of harm to the data subject.

The sensitivity of data may be regarded in light of the definition of “sensitive personal data” in Section 2 of the Act. This includes biometric data, race or ethnic origin, religious or similar beliefs, such as those reflecting conscience or philosophy, health status, sex life or sexual orientation, and political opinions or affiliations. The “unauthorized disclosure of or access to” such personal data may in some circumstances put a data subject at a high risk of discrimination, loss of reputation, embarrassment and financial loss. The risk may be higher if the racial or ethnic origin, religion or other beliefs are a minority and already adversely

treated in society. Some sexual orientation may be the subject of hostile social opinions, thus increasing the risk. Disclosure of a serious disease may result in the individual losing employment or being socially shunned. If such risk is high and not sufficiently mitigated, then the data controller must make the communication to the affected data subject.

The “destruction,” “loss” or “alteration” sensitive personal data may also result in a high risk of harm to a data subject if the data subject requires access to that data. For example, if a health care provider is unable to access a data subject’s medical records, the data subject may be at high risk of receiving inadequate treatment.

“Sensitivity” is not the only attribute of personal data that could lead to harm. For example, the destruction, loss, alteration or unauthorized disclosure of or access to certain financial information may by its nature be likely to result in a high risk of harm to affected data subjects. Release of bank account or similar information could increase the likelihood of theft or fraud. Similarly, unavailability of financial information could result in denial of services or an inability to conclude a transaction. In addition, the unauthorized disclosure of or access to personal data of children should generally be considered likely to result in a high risk to the rights and freedoms of those children, absent other factors to sufficiently mitigate that risk.

The scope of the personal data involved in the breach must also be considered. Some personal data in isolation is not likely to result in high risk to rights and freedoms, but the likelihood may increase as the data set grows. For example, in isolation, the unauthorized disclosure of a data subject’s name, date of birth, address, former residence, mother’s maiden name or tax ID number would probably not be likely to result in a high risk to rights and freedom. However, the unauthorized disclosure of all of these pieces of data in combination may result in a high risk of the data subject being the victim of identity theft or other fraudulent activity.

B. When may a public communication substitute for a required communication to a data subject?

Section 33(3)(b) of the Act provides that if a direct communication to a data subject required under Section 33(3)(a) of the Act “would involve disproportionate effort or expense or is otherwise not feasible,” the data controller may instead make “a public communication in one or more widely-used media sources such that data subjects are likely to be informed.” A data controller relying on this provision will need to document its analysis of the circumstances that led it to believe it could so rely.

Disproportionate effort or expense or otherwise not feasible

The Authority generally views “disproportionate effort or expense” as a high threshold to overcome, as most required communications are likely to require significant effort and/or expense when significant numbers of data subjects are affected. That said, the disproportionality of the effort or expense must be measured against:

- the likelihood and severity of risk to the rights and freedoms of the data subject; and
- the potential benefits of a direct notification to the data subject as opposed to public media communication to mitigate the harm.

If the unauthorized disclosure of sensitive personal data raises a high likelihood of a serious risk to the rights and freedoms of the data subject, the effort or expense of a direct communication must be very large indeed for the data controller only to make a public media communication. In the case of unauthorized disclosure of financial information, for example, a direct notification may alert the data subject to change passwords or other information to prevent becoming the victim of theft or fraud. The severity of the risk and great benefit of a direct communication means that the effort and expense would have to be very large to outweigh the benefit and justify only making a public media communication.

The Authority interprets "otherwise not feasible" to mean only that the data controller is unable to make a communication because the data controller no longer has or can obtain a means of contacting the data subject. This could be the case because the personal data was not obtained directly from the data subject or from a source that has the data subject's contact information, the contact information available is out of date, or the contact information is itself the subject of a personal data breach and no longer available to the data controller.

Public communication in one or more widely-used media sources

The public communication permitted under Section 33(3)(b) of the Act must be made in "one or more widely-used media sources such that data subjects are likely to be informed." In general, the Authority will consider it insufficient for a data controller to make the public communication in one media source or in one type of media source or to make the communication only once. For example, a single public communication in single newspaper is likely insufficient. However, recurring public communications made concurrently in many media sources, including newspapers, websites, social media, radio, television and billboards, is much more likely to inform the affected data subjects.

Whether affected data subjects are likely to be informed will also depend on the circumstances of the data subjects affected. For example, if all of the data subjects are within a single geographical region, the public communications should be tailored to media sources widely viewed in that region. If the data subjects are all members of a particular organization or other group, the public communications should be made in media sources that are popular with members of that organization or group or the data controller should enlist the organization or group itself to help disseminate the communication.

The data controller should think practically about what media and form of publication are genuinely likely to attract the attention of data subjects who are the subject of the breach and whose rights and freedoms are at high risk.

C. Content of communications to affected data subjects or public communications

Section 33(3)(a) of the Act requires that a direct communication to affected data subjects, or a public communication made in its place, should "communicate the personal data breach to the data subject." To achieve this objective, the controller should include in the communication:

- a description of the nature of the personal data breach, including the type of personal data records concerned;

- the name, contact details and a point of contact of the data controller;
- the likely consequences of the personal data breach to the affected data subjects; and
- a description of measures taken or proposed to be taken by the data controller to address the breach, including measures to mitigate its possible adverse effects on the affected data subjects.

Section 33(3)(a) of the Act further requires the data controller to "include measures the data subject could take to mitigate effectively the possible adverse effects of the data breach." For example, in the case of unauthorized disclosure of or access to personal data, a data controller may instruct a data subject to reset passwords, monitor activity in financial accounts, or contact service providers or counterparties to be alerted to fraud. In the case of destruction, loss or alteration of personal data, a data controller may suggest mechanisms whereby the data subject may recover the personal data from other sources.

In addition, a direct communication to affected data subjects, or a public communication made in its place, must be made using "plain and clear language." This means that the communication should be written in a manner that is easy for a lay person to understand, and thus the content may need to differ significantly from the notification made to the Authority. The communication must also be presented in an accessible format using easily readable font styles and sizes. In addition, if the affected data subjects are unlikely to speak English, the communication should be translated into appropriate languages.

D. Deadline for communications to affected data subjects or public communications

Section 33(3)(a) of the Act requires that a communication to an affected data subject be made "without undue delay." The Authority interprets this to mean as soon as reasonably possible after the notification to the Authority is made. The Authority applies the same deadline to a public communication if made in place of a direct communication to the affected data subjects under Section 33(3)(b) of the Act.

As set out in section 3.2(B) above, a data controller must indicate as part of its notification to the Authority whether it will make a communication to some or all of the affected data subjects or a public communication and provide a rationale for its decision. If the Authority disagrees with the rationale provided, it may issue an order compelling the data controller to make communications directly to the data subjects or to make a public communication. In that case, such communications must be made as soon as reasonably possible after the order is issued by the Authority.

If not provided in the notification to the Authority, the data controller must promptly submit to the Authority the text of the direct communications it has sent or intends to send to affected data subjects or the public communication it has made or intends to make once such text is finalized.

3.4. When will the Authority make its own public communication to affected data subjects

The Authority may determine that the text of a communication (whether submitted with the notification or subsequently) is insufficient and may order the data controller to make

additional communications. As set out in Section 33(6), the Authority may also, or instead, make its own public communication about the personal data breach to inform affected data subjects.

4. Record keeping

Section 33(9) of the Act requires every data controller and data processor to:

> *. . . keep a record of all personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in a manner that enables the Authority to verify compliance with this section.*

This record-keeping obligation applies to all personal data breaches, regardless of whether they led to a notification by a data controller to the Authority. In addition, the obligation extends to all of the risk assessments, decisions and other determinations described in these Guidelines that the data controller or data processor made, and copies of any communications with data subjects regarding the personal data breach. The Authority may require such records to be made available to it in the course of an investigation.

5. Simplified flowchart of data controller obligations