

Malawi Communications Regulatory Authority

Guidelines on Personal Data Breach Notifications and Communications

DRAFT

The Authority issues this document as a source of information and guide to data controllers and data 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

1. INTRODUCTION.....	2
1.1. Background	2
1.2. Purpose and application of the Guidelines	2
2. Personal data breaches	3
2.1. What is a personal data breach?	3
2.2. When does a data controller or data processor become aware of a personal data breach?	3
3. Required personal data breach notifications	4
3.1. Data processor notifications and obligations to respond to requests	5
A. Data processor notifications	5
B. Content of data processor notifications	5
C. Deadline for a data processor notification	6
3.2. Data controller notifications to the Authority	6
D. Content of notifications to the Authority	6
E. Deadline for a notification to the Authority	7
3.3. Data controller notification to affected data subjects	7
A. Under what circumstances is a notification to an affected data subject required?	7
B. When may a public notification substitute for a required notification to a data subject?	9
C. Content of notifications to affected data subjects	11
D. Deadline for notifications to affected data subjects	11
3.4. The Authority's public notification to affected data subjects	11
4. Record keeping	12
5. Simplified flowchart of data controller obligations	13

DRAFT

1. INTRODUCTION

1.1. Background

The Malawi Communications Regulatory Authority (hereinafter referred to as “the Authority”) as the designated Data Protection Authority is mandated by the Data Protection Act (No. 3 of 2024) (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.

The Act gives a data controller and data processor an obligation to notify in the event of a personal data breach. Section 36(1) requires that a data controller shall, in the case of a personal data breach, notify the Authority within seventy-two hours of becoming aware of the breach. Further, section 36(5) of the Act requires every data processor to notify the data controller when a personal data breach has occurred. It further requires every data controller to communicate to affected data subjects where there is a personal data breach that is of high risk to the rights and freedoms of the data subjects.

Section 5(2)(a) of the Act gives mandate to the Authority to develop and publish guidelines to promote data protection compliance. This guideline will provide guidance on all personal data breach notifications and communications.

1.2. Purpose and application of the Guidelines

This Guideline gives practical advice and guidance to data controllers and data processors when determining:

- whether a personal data breach has occurred;
- whether a personal data breach notification is required to be made to affected data subjects;
- the format and contents of any such required personal data breach notification ; and
- the deadline by which a required personal data breach notification 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 36 and Section 37 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 data security leading to, or likely to lead to, unauthorized disclosure of, or access to, or loss, alteration or accidental or unlawful destruction of personal data transmitted, stored or otherwise processed by the data controller or data processor.

The breach must involve personal data that is being processed by the data controller or data processor.

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

Ordinarily, the data controller shall notify the authority within 72 hours of becoming aware of the personal data breach. Similarly, the data processor shall also notify the data controller of a personal data breach with 72 hours of becoming aware of the data breach. The deadlines for notification of personal data breaches in Section 36(1) and (5) of the Act 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 the proviso to Section 35(1) of the Act and therefore has an appropriate capability to detect any reasonably anticipated personal data breaches.

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 the data controller or data processor has a reasonable degree of certainty that a personal data breach has occurred. Implicit in this standard is an obligation to

promptly and adequately investigate any suspected or known 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 36.

A data controller or data processor that engaged a data processor is deemed to have awareness of the breach upon receipt of a breach notification by the data processor it engaged. However, the data controller or data processor 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, the data controller or data processor 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

Section 36 and 37 of the Act sets out three distinct types of personal data breach notifications:

- data controller notifications to the Authority (Section 36(1));
- data processor notifications to data controller (Section 36(5)); and
- data controller notifications to affected data subjects (Section 37(1)).

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

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 36(5) of the Act:

- a data processor is ALWAYS required to notify a data controller 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.

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 obligates a data processor to notify an engaging entity if the personal data processed on the engaging entity's behalf is the subject of a personal data breach.

Even if a data processor learns of the personal data breach from its engaging entity, it is still required to notify the engaging entity under Section 36(5). 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 36(1).

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 36(2) 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.

3.2. Data controller notifications to the Authority

Under Section 36(1) of the Act:

- a data controller is required to notify the Authority when a personal data breach has occurred; and
- the notification must be made within 72 hours after the data controller becomes aware of the personal data breach.

D. Content of notifications to the Authority

Based on the requirements of Sections 36(2) of the Act, the following information should be conveyed in the notification to the Authority:

- a description of the nature of the personal data breach;
- where possible, a description of the categories of personal data affected by the breach;
- where possible, the number of data subjects affected by the breach;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed to be taken by the data controller to address the personal data breach; and
- the name and contact details of the data protection officer of the data controller.

Where it is not practically possible for a data controller to provide the information above within the prescribed period, the data controller shall provide the information as soon as the information becomes available. The data controller must provide to the Authority the reasons for failing to comply with the 72 hours deadline and further furnish the Authority with the practical steps the data controller is implementing to make the information available to the Authority.

In addition, a data controller must indicate whether it intends to make a communication to the affected data subjects by Section 37(1) or a public communication, as required in some circumstances by Section 37(4) of the Act. 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.

E. Deadline for a notification to the Authority

Section 36(1) of the Act requires a data controller to make its notification within 72 hours after becoming aware of the personal data breach.

3.3. Data controller notification to affected data subjects

Under Section 37(1) of the Act:

- a data controller is required to notify affected data subjects when a personal data breach has occurred, contingent upon the outcome of a risk assessment; and
- the notification must be made within 72 hours of the data controller becoming aware of the breach and
- where the notification involves a disproportionate effort or expense, the data controller shall make a public notification, in at least one newspaper of wide circulation in Malawi and any other mode of communication the data controller considers appropriate.

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

Section 37(1) requires a data controller to notify 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. Such risk assessment may lead to the conclusion that a notification ought to be made to the affected data subjects where the breach is of “high risk” to their rights and freedoms. This may depend on the specific personal data attributes, circumstances and vulnerabilities relating to the data subjects.

Factors to consider in the risk assessment

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 37(2) of the Act sets out three factors that a data controller may take into account when determining whether a notification 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;

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 so that it is not necessary to notify data subjects.

The second factor is:

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

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 “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. The data controller 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 category of the personal data involved.

The nature, scope, and category of the personal data involved in the breach is directly related to the risk of harm to the data subject.

For example, The Act provides for “sensitive personal data” in Section 2. This includes biometric data, race or ethnic origin, religious or similar beliefs, such as those reflecting conscience or philosophy, health status, and political opinions or affiliations. The “unauthorized disclosure of or access to” any such sensitive personal data may in some circumstances put a data subject at a high risk of discrimination, loss of reputation, embarrassment and financial loss. If such risk is high and not sufficiently mitigated, then the data controller must make the communication to the affected data subject.

The category of personal data 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 notification substitute for a required notification to a data subject?

Section 37(4) of the Act provides that if a direct notification to a data subject required under Section 37(1) of the Act “would involve disproportionate effort or expense,” the data controller may instead make “a public notification 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

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 notification 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 notification 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 notification means that the effort and expense would have to be very large to outweigh the benefit and justify only making a public media communication.

Public communication in one or more widely-used media sources

The public communication permitted under Section 37(4) 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 notifications to affected data subjects

Section 37(3) of the Act requires that a notification to affected data subjects, should “communicate the personal data breach to the data subject.” To achieve this objective, the controller should include in the notification:

- a description of the nature of the personal data breach,
- 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,

In addition, a direct notification to affected data subjects, or a public notification of the personal data breach, must be in “plain and clear language.” This means that the notification 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 notification 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 notifications to affected data subjects

Section 37(1) of the Act requires that a communication to an affected data subject be made within 72 hours of the data controller becoming aware of the breach.

3.4. The Authority’s public notification to affected data subjects

The Authority may make a public notification where it considers the measures taken by the data controller to be inadequate. Such public notification of the personal data breach may be circulated in at least one newspaper or any other mode of communication. Inadequate measures may include but not limited to delays in notifying data subjects of the personal data breach, insufficient risk assessments.

4. Record keeping

Section 36(4) of the Act requires every data controller and data processor to:

” a data controller shall, with respect to each personal data breach, keep a record of the breach and the information prescribed under subsection 2”

This record-keeping obligation extends to all 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

