x

'creating a level playing field'

CYBER AND DATA PROTECTION IMPLEMENTATION GUIDELINE ON DATA BREACH NOTIFICATION AND HANDLING

CDPG 3 OF 2024

1. PURPOSE AND EFFECTIVE DATE

This guideline is issued in terms of the mandate of the Authority under section 6 (1) (a) of the Cyber and Data Protection Act [*Chapter12:07*] (hereinafter referred to as "the CDPA") which provides for the function of the Authority to establish conditions for the lawful processing of data as read with section 19 of the CDPA on data and security breach notifications to the Authority. The guideline shall be read in conjunction with the provisions of the CDPA and the regulations. The guideline is effective from the date of publication.

2. INTRODUCTION

The guideline seeks to elaborate on the general provision relating to data breach notifications outlined in section 19 of the CDPA as read with the regulations. It gives general guidance to data controllers and data subjects on some of the frequently asked questions on data breach notifications and handling. It provides procedures for handling personal data breaches, to prevent recurrence and to mitigate the loss and damage caused to the data subjects involved.

3. WHAT IS PERSONAL DATA?

Section 3 of the CDPA defines personal information as data relating to a data subject which can be used for their personal identification and includes names, addresses, telephone numbers, race, national or ethnic origin, colour, religious or political beliefs or associations, age, sex, sexual orientation, marital status, family status, fingerprints, blood type, healthcare history, educational, financial, criminal or employment history among others. Data breach incidents often involve the personal data of individuals, such as customers, service users, employees, job applicants among many other individuals.

4. WHAT IS A DATA BREACH?

A data breach is a confirmed compromise of the security of personal data held by a data controller, which exposes the personal information of data subjects to the risk of unauthorised or accidental access, processing, erasure, loss, or use of their personal data. The following are some examples of data breaches:

4.1 The loss of personal data stored on devices such as laptop computers, USB flash drives, portable hard disks, or backup tapes.

4.2 The improper handling of personal data, such as improper disposal, sending of emails to unintended parties or the unauthorised access of databases by employees.

4.3 The hacking or unauthorised access of personal information by malicious actors.

4.4 The disclosure of personal data to a third party who obtained the data through social engineering or otherwise.

4.5 The leakage of data caused by the installation of file-sharing software on a computer or updates.

4.6 Failure by a data controller or processer to take appropriate technical and organisational measures that are necessary to protect data from negligent or unauthorised destruction, negligent loss, unauthorised alteration or access and any other unauthorised processing of the data as provided for under the CDPA.

4.7 The security measures must consider:

4.7.1 the sensitivity of data and the harm that could result if any mishaps should occur;

4.7.2 the physical location and cloud-based storage locations where the data is stored;

4.7.3 the media on which the data is stored;

4.7.4 any measures taken for ensuring the integrity, prudence and competence of persons having access to the data;

4.7.5 the need for the secure transmission of the data; and

4.7.6 the need to ensure the availability of data.

5. ENGAGEMENT OF A DATA PROCESSOR

In the event of a data controller engaging a data processor, whether within or outside Zimbabwe, the data controller must adopt contractual or other means, to prevent unauthorised or accidental access, processing, erasure, loss, or use of the data transferred to the data processor for processing.

6. CAUSES OF DATA BREACHES?

Data breaches can result from various factors which include:

6.1 Cyberattacks

Data controllers may fall prey to cyberattacks which may exploit vulnerabilities in their systems or networks for example ransomware, malware, brute force attacks, or phishing business emails can compromise, resulting in unauthorised access to, or even exfiltration of the personal data stored in their servers or databases.

6.2 System misconfigurations

System misconfigurations refer to errors or oversights in the setup or configuration of hardware, software, or network components within an informational technology infrastructure. These errors can lead to data breaches, such as unauthorised access to personal data through systems that lack authentication measures or proper access control mechanisms.

6.3 Loss of physical documents or portable devices

Data breaches often result from the loss of physical documents or storage devices containing sensitive data and occur when such items are misplaced, stolen, or improperly disposed of. For example, sensitive documents left unattended in public places or lost during transit can lead to unauthorised access and potential exposure of personal information. Similarly, storage devices like USB drives or portable hard disks that are misplaced or stolen may contain unencrypted data that could be accessed by unauthorised individuals. These incidents highlight the importance of secure handling, storage, and disposal practices to mitigate the risk of data breaches through physical loss.

6.4 Improper/wrongful disposal of personal data

Personal data stored in various formats, including hard disks, paper files, USB drives, and other storage devices, is at risk of being accidentally or improperly disposed of if proper document destruction practices are not followed. For instance, failing to shred paper

documents or securely wipe data from electronic devices before disposal can lead to data breaches. Unauthorised individuals may retrieve discarded documents or devices, potentially gaining access to sensitive information such as personal information and financial records among others.

6.5 **Inadvertent disclosure by email or by post**

Personal data, whether stored in digital files or physical documents, can inadvertently be sent to unintended recipients due to human error or technical glitches in communication systems. Such incidents can occur when emails are misaddressed, or documents are mistakenly included in correspondence. As a result, attachments containing personal data may be accessed by individuals who lack authorisation, potentially leading to privacy breaches or exposure of sensitive information.

6.6 **Insider threats**

This mainly entails malicious actions perpetrated by authorised personnel within an organisation, including employees or contractors, who exploit their privileges to unlawfully acquire, mishandle or disclose sensitive data.

6.7 **Third-Party vulnerabilities**

Third-party vulnerabilities are weaknesses or security risks that arise from external entities or organisations that are not directly part of the primary organisation's operations but have access to its systems, data, or networks such as service providers or contractors.

6.8 **Human error**

Mistakes made by employees or individuals, such as sending sensitive information to the wrong recipient, improper disposal of documents, or accidental exposure of data due to misconfigured settings.

7. DATA BREACH RESPONSE PLAN

Every data controller must have a data breach response plan. A data breach response plan outlines the data controller's course of action in the unfortunate event of a data breach. An extensive data breach response plan is crucial for promptly addressing and efficiently handling data breaches. The plan should clearly outline a comprehensive set of procedures to be followed in the event of a data breach. It should also detail the data controllers' strategy for effectively identifying, containing, assessing, and managing the impact of the incident from beginning to end. Responding promptly to a data breach can greatly reduce and control the impact of the breach.

8. WHAT TO INCLUDE IN A DATA BREACH RESPONSE PLAN?

It is recommended that a plan should cover the following critical aspects:

8.1 A description of what constitutes a data breach with examples tailored to the nature of the organisation, and the criteria that trigger the implementation of the data breach response plan.

8.2 An internal incident notification procedure to escalate the breach to senior management, the Data Protection Officer and/or dedicated data breach response team, incorporating a standard form to facilitate the reporting of the required information.

8.3 A data breach response team: The designation of the roles and responsibilities of members of the dedicated data breach response team. The Data Protection Officer shall assume overall responsibility for notifying the Authority and the data subjects of the data breach; the Information Security/Technology department for identifying the location of potentially compromised data and taking remedial technical measures.

8.4 A contact list with contact details of all breach response team members (for example, the core management, Data Protection Officer, Information Technology experts, and Risk Management.

8.5 A risk assessment workflow to assess the likelihood and severity of the harm caused to the affected data subjects as a result of the breach. The risk of harm to the data subject refers to the potential negative consequences that individuals may face if their personal data is compromised or accessed by unauthorized parties. This risk can vary depending on the sensitivity and nature of the data involved.

8.6 A containment strategy for preventing further unauthorised access and mitigate any potential harm caused by the data breach. This may include isolating affected systems, changing access credentials, applying patches to vulnerabilities, or implementing additional security measures.

8.7 A communication plan covering the criteria on how the affected data subjects, Data Protection Authority and other relevant parties will be notified, the kind of information that must be provided, the point of contact in the organisation responsible for liaising with the stakeholders and the methods of notification.

8.8 An investigation procedure for determining what data was compromised that include how the breach occurred including gathering and preserving evidence, conducting a root cause analysis, and identifying the full extent of the breach. The procedure may include:

i. Gathering all evidence related to the breach, including logs, system snapshots, emails, and any other relevant data.

ii. Preserving evidence in its original state to maintain its integrity for potential legal proceedings.

iii. Documenting every action taken to maintain a chain of custody.

iv. Conducting a thorough analysis to determine the root cause of the breach. This may involve examining system logs, network traffic, and application vulnerabilities.

v. Identifying the full extent of the breach, including the number and types of affected data subjects and the specific data compromised.

8.9 A record-keeping policy to ensure that the incident is properly documented as the relevant records may be required by regulatory authorities or law enforcement agencies. This will be used for cross referencing in the future.

8.10 A post-incident review mechanism for identifying areas that require improvement to prevent future recurrence.

8.11 A continuous training program or drill schedule to guarantee that all personnel are ready to implement the response plan proficiently in the event of a data breach.

9. HANDLING DATA BREACHES

The proper handling and management of data breaches demonstrates the data controller's commitment to tackling the problem and may substantially reduce the impact of a breach on affected individuals and the potential reputational damage to the organisation. The following steps are recommended when handling data breaches:

9.1 Immediate gathering of essential information

As a starting point, the data controller shall promptly gather all relevant information of the data breach to assess the impact on data subjects and to identify appropriate mitigation measures. Questions such as the following should be addressed:

9.1.1 When did the breach occur?

9.1.2 Where did the breach occur?

9.1.3 How was the breach detected and by whom?

9.1.4 What was the cause of the breach?

9.1.5 What kind of personal data was involved?

9.1.6 How many data subjects might be affected?

9.1.7 What harm may have been caused to the affected individuals?

9.2 The staff members who first discover the breach should escalate the incident to the Data Protection Officer, according to the procedures laid down in the data breach response plan.

10. CONTAINING DATA BREACHES

After detecting the breach and conducting an initial assessment, the data controller should immediately take steps to contain the breach as effectively as possible. Remedial actions to lessen the harm or damage that may be caused to the affected data subjects should be taken. Containing a data breach involves several crucial steps to prevent further unauthorised access and minimise its impact.

11. ASSESSING THE RISK OF HARM

11.1 Once all essential information has been gathered, the controller should then ensure that they understand the risks of harm that may be caused to the affected individuals, so that they can take steps to limit the impact. The possible harm caused by a data breach may include:

11.1.1 Threats to personal safety.

11.1.2 Identity theft.

11.1.2 Financial loss.

11.1.4 Humiliation or loss of dignity, damage to reputation or relationships.

11.1.5 Loss of business or employment opportunities.

11.2 The result of an assessment may reveal a real risk of harm, such as potential threats to the security and confidentiality of sensitive information. This could include scenarios where personal data is vulnerable to unauthorised access or exposure, leading to possible identity theft, financial loss, or reputational damage for affected individuals and the organisation.

11.3 On the other hand, a data breach assessment may reveal a lower risk of harm, for example,

the loss of a USB flash drive containing securely encrypted data which may not be sensitive in nature, or when the lost or misplaced device containing personal data has subsequently been found and the personal data does not appear to have been accessed.

11. NOTIFICATION TO THE AUTHORITY

Section 19 of the CDPA provides that a data controller shall notify the Authority in writing within twenty-four (24) hours after becoming aware of an actual or suspected data breach. The data controller is required to report the breach using form DP3 provided for in the regulations,

12. CONTENTS OF A DATA BREACH NOTIFICATION

12.1 A data breach notification is a formal written notification given by the data controller to the Authority, the affected data subjects, and law enforcement agencies where the breach constitutes a criminal offense. The data controller is required to notify the Authority within twenty-four (24) hours of becoming aware of the breach as provided for in terms of Section 19 of the CDPA. The notification to the Authority must be made regardless of the progress of any internal investigation. If the data controller is initially unable to provide full details about the breach, providing as much information as possible in the notification is still desirable. After the full details of the incident are revealed, all information should be submitted to the Authority and other law enforcement agencies without delay.

12.2 The data breach notification should include the following details:

12.2.1 A general description of what occurred.

12.2.2 The date and time of the breach and its duration (or an estimate).

12.2.3 The date and time when the breach was detected.

12.2.4 The source of the breach (either the data user or the third party that processed the personal data on its behalf).

12.2.5 Basic information about the type of breach.

12.2.6 A list of the types of personal data involved.

12.2.7 The categories and approximate number of data subjects involved.

12.2.8 The categories and approximate number of personal data records involved.

12.2.9 An assessment of the risk of harm (such as identity theft or fraud) that could result from the breach.

12.2.10 A description of the measures taken or to be taken to mitigate the loss or to prevent further unauthorized access to and/or leakage of personal data.

12.2.11 The contact information of the Data Protection Officer (DPO).

12.2.12 Information and advice on the actions the data subjects can take to protect themselves from any adverse effects of the breach and from identity theft or fraud (e.g., resetting passwords, being alerted to phishing emails or fraudulent activity on their accounts, contacting financial institutions to change their credit card details, requesting that credit reference agencies suspend any provision of their credit reports to third parties.

13. HOW TO SUBMIT THE NOTIFICATION TO THE AUTHORITY

Data controllers shall notify the Authority of data breaches in writing through submission of a completed Data Breach Notification Form (DP3) and the communication shall be addressed to the Director-General. The notification can be submitted by email through the following email dataprotectionunit@dpa.zw or the.regulator@potraz.zw. Oral notifications are not acceptable.

14. NOTIFICATION OF THE DATA SUBJECT

If the data breach is likely to result in a real risk of harm to the affected data subjects, they should be informed within 72 hours. The data subjects can be notified directly by phone, in writing, via email or in person. When a direct data breach notification is not practicable in the circumstances, for example, if data subjects are not immediately identifiable or if public interest exists, then public announcements, newspaper advertisements or announcements on websites or social media platforms may be more effective. If a data breach results in particularly serious harm or affects a large number of individuals, using multiple methods to publicise the breach is a reasonable approach.

15. DOCUMENTING BREACHES

A data controller should learn from the data breach incident, facilitate a post-breach review, and improve personal data handling practices as appropriate. A comprehensive record of the incident is therefore required, which should include all facts relating to the breach, including details of the breach and its effects as well as the containment and remedial actions taken by the data controller. Organisations that are required to comply with the laws and regulations of other jurisdictions should also consider whether there are any mandatory documentation requirements under those laws and regulations.

16. SUBMISSION OF FINAL INVESTIGATION REPORT

The data controller is required to submit a final report of the investigation to the Authority within 21 days of reporting the breach.

17. PENALTIES

A data controller who fails to:

(a) report data breaches within the prescribed timeframe without a just cause.

(b) cooperate with the Authority in conducting enquiries or investigations relating to data breaches.

(c) respond to information requests on data breaches within 14 days.

(d) conclude data breach investigations and submit a report within 21 days from the date of notification.

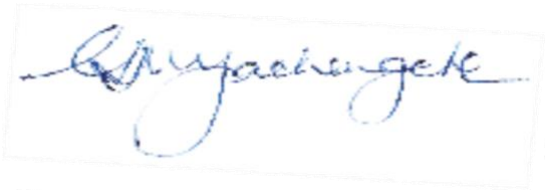
(e) put in place adequate security.

Shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a

period not exceeding 7 years or to both such fine and such imprisonment.

For complaints and further guidance, contact the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) on dataprotectionunit@dpa.zw; regulator@potraz.zw or call +263 242 333032/46/48.

ISSUED ON THIS 13th DAY OF NOVEMBER 2024.



_____
POTRAZ DIRECTOR GENERAL