'creating a level playing field'

CYBER AND DATA PROTECTION IMPLEMENTATION GUIDELINES ON APPOINTMENT, ROLES, RESPONSIBILITIES, TRAINING AND CERTIFICATION OF DATA PROTECTION OFFICERS

CDPG 1 OF 2024

1. PURPOSE AND EFFECTIVE DATE

These guidelines are issued in accordance with section 20(6) of the Cyber and Data Protection Act [Chapter 12:07] (hereinafter referred to as "the CDPA") which provides that the "Authority shall provide guidelines that provide for the duties, qualifications and functions of the data protection officer…" These guidelines seek to assist data controllers and data protection officers to discharge their obligations as stipulated in the CDPA. The guidelines shall be read in conjunction with the provisions of the CDPA and Regulations. The guidelines are effective from the date of publication.

2. INTRODUCTION

The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) is the designated Data Protection Authority of Zimbabwe. According to Section 20(6) of the CDPA, POTRAZ has a legal obligation to come up with guidelines that provide for the qualifications and functions of Data Protection Officers. These guidelines repeal POTRAZ Regulatory Notice 1 of 2022.

3. APPOINTMENT OF A DATA PROTECTION OFFICER (DPO)

Section 3 of the CDPA defines a Data Protection Officer (hereinafter referred to as a DPO) as any individual appointed by the data controller and is charged with ensuring, in an independent manner, compliance with the obligations provided for in the CDPA. The CDPA also defines a data controller as any person who determines the purpose and means of processing data and is licensable by the Authority, including public bodies, private institutions and non-governmental organisations. Processing of data performed by the controller, includes collection, organisation, adaptation, transfer, alteration, storage, retrieval, erasure and destruction of the data among other operations.

3.1 Data controllers shall appoint a DPO within ninety (90) days from the date of promulgation of the Cyber and Data Protection Regulations (CDPR).

3.2 The data controller shall notify the Authority within forteen (14) days of the appointment, resignation or termination of contract of the incumbent DPO.

3.3 The data contoller shall re-appoint a DPO within ninety (90) days of the date of termination of contract of the incumbent DPO.

3.4 Data controllers processing personal data prior to the promulgation of the CDPA **shall** appoint a DPO to comply with the Act.

4. IS IT MANDATORY TO APPOINT A DPO?

It is mandatory for a data controller to appoint a DPO as provided in S20 (4)(b) of the CDPA and S12(1) of the CDPR.

4.1 **A data controller is required to appoint a DPO where:**

4.1.1 the processing is carried out by a public authority or body.

4.1.2 the core activities of the data controller or the processor consist of large-scale data processing operations, which require regular and systematic monitoring of data subjects: or

4.1.3 the core activities of the data controller or the processor consist of processing of special or sensitive categories of data.

4.2 Who is exempted from appointing a DPO

A data controller who processes personal data for personal, household, family, law enforcement, journalistic, historical or archival purposes is exempted from appointing a data protection officer. Personal, household and family purposes include but are not limited to:

4.2.1 Social networking or managing family-related social media groups, sharing home/ family gathering photos, personal phone books (contacts), or

4.2.2 Personal use groups to keep in touch with acquaintances, school association groups, neighbourhood update groups, hobbyists, where data is used for purely private, domestic, household, or familial reasons with no connection to a business activity or transaction, or

4.3.3 Any other personal, family or household affairs not connected to commercial, business, or professional activities.

A data controller who processes personal data for less than 50 data subjects is excluded from appointing a DPO.

NB: While the above categories maybe exempted from appointing a DPO, they are required to abide by the data protection principles to safeguard the personal data that they collect.

5. PUBLICATION OF THE DPO's DETAILS

5.1 The DPO shall be the contact point with respect to data subjects, the Authority and within the data controller's organisation. It is imperative that all the mentioned stakeholders have the relevant and up to date information relating to the DPO. The data controller is obliged to:
publish the details of the appointed DPO on the controller's websites or notice boards.

5.1.1 notify the Authority in writing of the appointment of their DPO.

5.1.2 notify the Authority of the change of DPO's contact details within a period of 14 days of such change.

6. THE POSITION OF THE DPO

6.1 Can an organisation have more than one DPO?

An organisation may, according to its structure and needs, have a team of people carrying out the various functions of the DPO, however, there must be specific people whose details are registered with the Authority and appointed as the DPO.

6.1.1 The provisions of the CDPA do not define whether a data controller must have a single or separate DPO for each of its subsidiaries. The data controller is responsible for determining this for example, a single DPO may be selected for numerous subsidiaries, taking into consideration the organisational structure and size.

6.1.2 If a data controller has appointed a single DPO, that person should be immediately accessible to all subsidiaries or business units. The concept of accessibility refers to convenient availability of the DPO as a contact point for data subjects, the Authority, and the internal customers within the organisation, given that one of the DPO roles is to inform and advise the controller and employees who process personal data of their obligations.

6.2.3 The DPO, with the help of a team, where necessary, must be able to efficiently communicate with data subjects. The availability of a DPO, whether physically on the same premises as employees or via a hotline or other secure means of communication, is essential to ensure that data subjects can contact the officer.

6.2.4 Given that the DPO is in charge of a wide range of tasks, it is the controller or processor's obligation to ensure that where a DPO is appointed to oversee multiple subsidiaries, with or without the help of teams, the duties are efficiently and effectively executed.

6.3 Can an existing employee be appointed as a DPO?

6.3.1 A DPO can be an existing employee if the professional duties of the employee are compatible with the duties of the DPO and do not result in a conflict of interest.

6.3.2 A DPO cannot hold a position within an organisation that leads him or her to be involved in the day to day running of core business operations, implementation of controls and determining the means of the processing of personal data.

6.3.3 The DPO is charged with ensuring, in an independent manner, compliance with the obligations provided in the CDPA.

6.3.4 The organisation shall determine whether or not the duties of the internal staff selected conflict with that of the DPO. If the internal staff member does not determine the purposes and means of the processing of personal data of the data subjects concerned and has the relevant skills and expertise as mentioned above, then he/she may be appointed as the DPO of the organisation, otherwise another person should be appointed, recruited or outsourced.

6.4 Can a Data Controller outsource or subcontract the role of the DPO?

A data controller may outsource the role of a DPO to a trained and certified individual. The appointment shall be based on a service contract. The obligations of the externally appointed DPO are the same as those of an internally appointed DPO.

6.5 Can a foreigner be a Data Protection Officer?

A DPO can be a foreigner provided that he/she is able to perform his/her duties in accordance with the CDPA and is trained, certified and registered by the Authority.

7. QUALIFICATIONS OF A DPO

7.1 Personal attributes

The DPO must be honest with high professional ethics. They must be an independent thinker and be able to exercise good judgement.

7.2 **Relevant skills and expertise of the DPO shall include, but are not limited to:**

7.2.1 expertise in local data protection laws and practices including an in-depth understanding of the CDPA.

7.2.2 an in-depth understanding and knowledge of how their organisation processes personal data.

7.2.3 an understanding of information technologies and data protection frameworks.

7.2.4 thorough knowledge of the operations of the organisation or entity.

7.2.5 ability to promote a data protection culture within the organisation.

7.2.6 possession of a data protection certificate issued by the Authority.

8. FUNCTIONS AND ROLES OF THE DPO

The DPO shall work in an independent manner, report to the highest level of management and have adequate resources to enable the controller to meet its obligations under the CDPA.

8.1 **Duties of a DPO include:**

8.1.1 Ensuring compliance by the data controller with the provisions of the CDPA, regulations, notices, directives and guidelines.

8.1.2 Dealing with requests made to the data controller by the Authority pursuant to the CDPA.

8.1.3 Informing and advising the employees about their obligations to comply with the CDPA and other data protection directives and notices.

8.1.4 Monitoring compliance with the Act and other data protection laws, and with organisational data protection polices, including managing internal data protection.

8.1.5 Raising awareness of data protection issues, training staff, and conducting internal audits.

8.1.6 Advising on and monitoring of data protection impact assessments.

8.1.7 Reporting and cooperating with the Authority in cases of data breaches.

8.1.8 Being the first point of contact with the Authority, and for data subjects in cases of data breaches or data subject access requests.

9. RESOURCES TO BE PROVIDED TO THE DPO BY CONTROLLER

9.1 The DPO must be availed with the resources necessary to enable him/her to carry out his or her tasks. The following resources must be provided to the DPO regardless of the nature of the processing operations and size of the organisation:

9.1.1 independence in the performance of their functions;

9.1.2 active support by senior management;

9.1.3 sufficient time to fulfil their tasks;

9.1.4 adequate financial resources, infrastructure (premises, facilities, equipment) and staff where necessary;

9.1.5 access to any essential support/ services within the organisation that enable the DPO to perform his/her duties effectively; and

certification and continuous capacity development.

10. LIABILITY OF THE DPO

10.1 Data protection compliance is the responsibility of the data controller. DPOs are not personally responsible for non-compliance with data protection requirements by the data controller.

10.2 Section 33(2) of the CDPA excludes the DPO from liability for non-compliance with the CDPA.

10.3 The data controller is required to ensure and be able to demonstrate that processing is performed in accordance with the CDPA. Therefore, even though the DPO is responsible for assisting the data controller in monitoring internal compliance, the DPO is not personally liable for any non-compliance with the CDPA by the data controller.

10.4 DPOs should not be dismissed or penalised by the data controller for performing their tasks.

11. TRAINING AND CERTIFICATION

11.1 Data Controllers must ensure that their DPOs are trained and certified by the Authority, or any institution accredited by the Authority, within six (6) months of promulgation of the Regulations.

11.2 Such training and certification will ensure compliance by the data controller with the requirements of section 20(5) of the CDPA.

11.3 Data Controllers must ensure that their DPOs attend annual professional development programmes organised by the Authority or by organisations approved by the Authority.

12. PENALTIES FOR NON COMPLIANCE

A data controller who fails

12.1 to appoint a data protection officer within ninety (90) days of promulgation of the regulations as per Section 12 (6) or

12.2 to notify the Authority of the appointment of the DPO in writing

shall be guilty of an offence and liable to a fine not exceeding level 7, a prison sentence of up to two years, or both a fine and imprisonment.

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

ISSUED ON THIS 13th DAY OF NOVEMBER 2024

POTRAZ DIRECTOR GENERAL