GENERAL NOTICE NO. 7/2023

THE ESWATINI DATA PROTECTION AUTHORITY (EDPA) ADVISORY GUIDELINES ON THE APPOINTMENT OF DATA PROTECTION OFFICERS

In March 2022 the Data Protection Act was passed to provide for the collection, processing, disclosure, and protection of personal information. The Act designates the Eswatini Communications Commission as the Eswatini Data Protection Authority (EDPA) charged with the mandate to administer and foster compliance to the Act.

Section 48(1) of the Act provides that "The head of a data controller may, subject to this Act, by order designate one or more officers or employees to be Data Protection Officers of that controller, to exercise, discharge or perform any of the power, duties or functions of the head of the data controller under this Act". Pursuant to this provision, the EDPA has therefore published advisory guidelines for the appointment of Data Protection Officers.

The Advisory Guidelines are available on the Commission's websites; www.esccom.org.sz and www.edpa.org.sz.

ESWATINI COMMUNICATIONS COMMISSION

(ESWATINI DATA PROTECTION AUTHORITY)

SUBJECT: ADVISORY GUIDELINES ON THE APPOINTMENT OF DATA PROTECTION OFFICERS

DATE: 28 NOVEMBER 2023

Preamble

WHEREAS the Eswatini Constitution values the dignity of every human person and guarantees full respect for the right to privacy.

WHEREAS the Data Protection Act of 2022 (DPA), guarantees the protection of personal information and rights of data subjects while ensuring free flow of information to promote innovation and growth.

WHEREAS Section 48(1) of the Act provides that "The head of a data controller may, subject to this Act, by order designate one or more officers or employees to be Data Protection Officers of that controller to exercise, discharge or perform any of the power, duties or functions of the head of the data controller under this Act"

WHEREAS pursuant to Section 5 of the Data Protection Act 2022, the EDPA is charged with the administration and implementation of the provisions of the law, which includes ensuring compliance with the provisions of the DPA and with international standards for data protection, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country, in coordination with other government agencies and the private sector.

WHEREAS in consideration of the foregoing premises, the EDPA hereby issues this Guideline to guide on the designation of a DPO:

Power to issue Guidelines

(1) This Guideline is made in accordance with Section 5(1)(y) of the Data Protection Act 2022 which empowers the Commission to "make such decisions and authorizations as may be necessary in carrying out the functions of the Commission".

Citation and Commencement

(2) This Guideline may be cited as the "EDPA Advisory Guideline on the Appointment of Data Protection Officers, 2023"

(3) This Guidelines shall come into force on 1 December 2023

Scope and Purpose of the Guideline

(4) (1) These Guidelines shall apply to all Data Processors and Data Controllers engaged in the processing of personal data as envisaged under Section 3 of the Data Protection Act 2022.

(2) This Guideline is premised on:

(a) The Data Protection Act, 2022

(b) International best practice: General Data Protection Regulation (GDPR)

Interpretation

(5) In this Guideline, the following terms shall have their respective meanings as hereinafter set forth: "**Act"** or **"DPA"** means the Data Protection Act, No 5. of 2022.

"**Commission"** means the Eswatini Communications Commission, established by the Eswatini Communications Commission Act No. 10 of 2013.

"**Conflict of Interest**" means a scenario wherein a DPO is charged with performing tasks, duties, and responsibilities that may be opposed to or could affect their performance as DPO. This includes, inter alia, holding a position within the Data Controller or Data Processor that leads him to determine the purposes and the means of the processing of personal data.

"**Data controller**" means a public or private body which or any other person designated by law, who alone or together with others, determines the purpose of and means for processing personal information, regardless of whether or not such data is processed by that party or by a data processor on its behalf, where the purpose and means of processing are determined by law;

"**Data processor**" refers to a natural or legal person, or public body which processes personal information for and on behalf of a data controller and under the instructions of a data controller, and excludes persons who are authorised to process data under the direct authority of a data controller;

"**Data Protection by Design**" means an approach to the development and implementation of projects, programs, and processes that integrates into the latter's design or structure safeguards that are necessary to protect and promote data protection, such as appropriate organizational, technical, and policy measures;

"**Data Protection Impact Assessment**" or "DPIA" means a process undertaken and used to evaluate and manage the impact on data protection of a particular project, program, process,

or measure;

"**Data Protection Officer**" or "**DPO**" means a person appointed by a data controller charged with ensuring compliance with this Act.

"**Data Sharing Agreement**" means a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties: provided, that only data controllers shall be made parties to a data sharing agreement.

"**Data subject**" means a person who is the subject of the processing of personal information and who is identified or identifiable;

"Entity" or "**Entities**" means a natural (individual) or legal person, public authority, agency or other body that processes (handles) Personal Data.

"**Eswatini Data Protection Authority or EDPA**" means the Eswatini Communications Commission charged with the mandate to administer and foster compliance to the Act as provided under Section 5 of the Act

"**Personal data or information**" means information about an identifiable individual that is recorded in any form, including without restricting the generality of the foregoing -

(a) information relating to the race, national or ethnic origin, religion, age, or marital status of the individual.

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved.

(c) any unique identifying number, symbol or other assigned to the individual.

(d) the address, fingerprints, or blood type of the individual.

(e) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual.

(f) correspondence sent to a data controller by the individual that is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence; and

(g) the views or opinions of any other person about the individual.

"**processing**" means an operation or activity or any set of operations, whether or not by automatic means relating to –

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as blocking, degradation, erasure, or destruction, of information.

"Sensitive Personal Data" means –

(a) genetic data, data related to children, data related to offences, criminal sentences or security measure, biometric data as well as, if it is processed for what it reveals, personal information revealing racial or ethnic origin, political opinions, or affiliations, religious or philosophical beliefs, affiliation, trade-union membership, gender, and data concerning health or sex life; or
(b) any personal information otherwise considered by the laws of Eswatini as presenting a major risk to the rights and interests of the data subject, in particular unlawful or arbitrary discrimination.

General Principles

(6) (1) These Guidelines shall be governed by the following general principles:

(a) The responsibility for complying with the Act, directives and/or decisions by the EDPA, and all other applicable laws lies with the Data controller or Data processor.
(b) The DPO shall act independently in the performance of their functions and shall enjoy sufficient degree of autonomy. For this purpose, the DPO must not receive instructions from the Data controller or Data Processor regarding the exercise of their tasks.
(c) The DPO is bound by secrecy or confidentiality concerning the performance of their tasks.

Mandatory Designation

(7) A Data controller or Data processor shall designate a person who shall function as a DPO. The DPO shall be accountable for ensuring the compliance by the Data Controller or Data Processor with the DPA, directives and/or decisions by the EDPA, and other applicable laws and regulations

relating to privacy and data protection.

General experience

(8) (1) The DPO should have the below general expertise:

(a) specialized knowledge and demonstrate reliability necessary for the performance of their duties and responsibilities.

(b) have expertise in relevant privacy or data protection policies, regulations, laws, and practices.

(c) have sufficient understanding of the processing operations being carried out by the Data Controller or Data Processor, including the latter's information systems, data security and/or data protection needs.

(d) have sufficient knowledge of the Data Controller or Data Processor business, sector in which it operates or field, and the latter's internal structure, policies, and processes.

(e) minimum qualifications for a DPO shall be proportionate to their functions, as provided in this Guideline.

Position of the DPO

(9) (1) The DPO may, inter alia:

(a) be a full-time employee of the Data Controller or Data Processor.

(b) Should be accorded autonomy and independence to fulfil their duties

(c) Where the employment of the DPO is based on a contract, the term or duration thereof should at least be two (2) years to ensure stability.

(2) In the event the position of DPO is left vacant, the Data Controller or Data Processor should provide for the appointment, or hiring of their replacement within a reasonable time not exceeding 3 months.

(3) The Data Controller or Data Processor may also require the incumbent DPO to occupy such position in a holdover capacity until the appointment or hiring of a new DPO, in accordance with the Data Controller or Data Processor internal policies or the provisions of the appropriate contract.

Outsourcing or Subcontracting of Functions

(10) (1) A Data Controller or Data Processor may outsource or subcontract the functions of its DPO. However, to the extent possible, the Data Controller or Data Processor must oversee the performance of their functions by the third-party service provider or providers.

(2) The DPO shall also remain the contact person of the Data Controller or Data Processor vis-

à-vis the EDPA. In addition, the overall DPO function remains the management's responsibility.

Independence, Autonomy and Conflict of Interest

(11) (1) A DPO must be independent in the performance of their functions and should be accorded a significant degree of autonomy by the Data Controller or Data Processor.

(2) In his or her capacity as DPO, a person may perform (or be assigned to perform) other tasks or assume other functions that shall not give rise to any conflict of interest.

Duties and Responsibilities of the DPO

(12) (1) The head of a data controller may, subject to this Act, by order designate one or more officers or employees to be Data Protection Officers of that controller to exercise, discharge or perform any of the power, duties, or functions of the head of the data controller under this Act. A data protection officer's responsibility shall include, without limitation –

(a) promoting compliance by the controller, with controller's obligations under this Act;

(b) dealing with requests made to the controller pursuant to the controller's obligations under this Act;

(c) cooperating with the Commission in relation to investigations or proceedings conducted in relation to the controller;

(d) pursuing legal appeals with relevant judicial authorities;

(e) develop and implement an organisation's Data Protection Management Programme (DPMP) in accordance with the DPA requirements that covers policy, processes, and people for handling of personal data at each stage of the data lifecycle;

(f) promote a culture of data protection and compliance across all units of the organisation;

(g) be responsible for data subjects' requests and dealing with requests made to the controller pursuant to the controller's obligations under this Act;

(h) be responsible for notifications to the EDPA in terms of the ACT, cooperating with the Commission in relation to investigations or proceedings conducted in relation to the controller; and pursuing legal appeals with relevant judicial authorities;

(i) monitor the Data Controller or Data Processor compliance with the DPA, directives and/or decisions by the EDPA and other applicable laws and policies. For this purpose, the DPO may:

(1) collect information to identify the processing operations, activities, measures, projects,

programs, or systems of the Data Controller or Data Processor, and maintain a record thereof.

(2) analyse and check the compliance of processing activities, including the directives and/or decisions of security clearances to and compliance by third-party service providers.

(3) inform, advise, and issue recommendations to the Data Controller or Data Processor.

(4) ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and

(5) advise the Data Controller or Data Processor as regards the necessity of executing a Data Sharing Agreement with third parties and ensure its compliance with the DPA requirements.

(j) advise on when and how Data Protection Impact Analysis (DPIA) are conducted to identify, assess, and address data protection risks, based on the organisation function's relative to activities, measures, projects, programs, or systems of the Data Controller or Data Processor;

(k) enhance compliance processes based on an evaluation of gaps in business operations and data protection requirements and clarify on ethically questionable situations at various stages of data or information life cycle;

(l) advise the Data Controller or Data Processor regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification, or deletion of personal data);

(m) develop incident management procedures and synthesis incident related analysis to distil key insights, resolve incidents and establish mitigating and preventive solutions;

(n) ensure proper data breach and security incident management by the Data Controller or Data Processor, including the latter's preparation and submission to the EDPA of reports and other documentation concerning security incidents or data breaches within the prescribed period;

(o) develop training programme to inform and cultivate awareness on privacy and data protection within the organization of the Data Controller or Data Processor, including all relevant laws, rules and regulations and directives and/or decisions s of the EDPA;

(p) advocate for the development, review and/or revision of policies, Guidelines, projects and/or programs of the Data Controller or Data Processor relating to privacy and data protection, by adopting a data protection by design approach;

(q) facilitate and guide stakeholders to apply design thinking methodologies and processes for

the organisation;

(r) develop a stakeholder engagement plan to serve as the contact person of the Data Controller or Data Processor vis-à-vis data subjects, the EDPA and other authorities in all matters concerning data privacy, protection, or security issues or concerns;

(s) cooperate, coordinate, and seek advise of the EDPA regarding matters concerning data privacy and security, and protection;

(t) perform other duties and tasks that may be assigned by the Data Controller or Data Processor that will further the interest of data privacy and security and uphold the rights of the data subjects.

(2) The DPO must have due regard for the risks associated with the processing operations of the Data Controller or Data Processor, taking into account the nature, scope, context, and purposes of processing. Accordingly, the DPO must prioritize their activities and focus their efforts on issues that present higher data protection risks.

General Obligations of the Data Controller or Data Processor Relative to the DPO

(13) (1) The Data Controller or Data Processor should:

(a) effectively communicate to its personnel, the designation of the DPO and their functions.

(b) allow the DPO to be involved from the earliest stage possible in all issues relating to privacy and data protection.

(c) provide sufficient time and resources (financial, infrastructure, equipment, training, and staff) necessary for the DPO to keep himself or herself updated with the developments in data privacy and security and to carry out their tasks effectively and efficiently.

(d) grant the DPO appropriate access to the personal data it is processing, including the processing systems.

(e) where applicable, invite the DPO to participate in meetings of senior and middle management to represent the interest of privacy and data protection.

(f) promptly consult the DPO in the event of a personal data breach or security incident; and ensure that the DPO is made a part of all relevant working groups that deal with personal data processing activities conducted inside the organization, or with other organizations.

Protections

(14) To strengthen the autonomy of the DPO and ensure the independent nature of their role in the organization, a Data Controller or Data Processor should not hinder, influence, intimidate, the DPO in the exercise of their function.

Contact Details of the DPO

(15) (1) To ensure that its own personnel, the data subjects, the EDPA, or any other concerned party, can easily, directly, and confidentially contact the DPO, the Data Controller or Data Processor may publish the DPO's contact details as follows:

(a) Website.

(b) Social media platforms

(c) Dedicated contact form

(2) A Data Controller or Data Processor may introduce or offer additional means of communicating through brochures and dedicated hotlines etc. For this purpose, the contact details of the DPO should include the following information.

(a) Title or designation

(b) Postal address

(c) A dedicated telephone number

(d) A dedicated email address

(3) The name or names of the DPO need not be published. However, it should be made available upon request by a data subject or the EDPA.

Accountability

(16) It remains the responsibility of the Data Processor and Data Controller and not that of the DPO, to comply with the DPA directives and/or decisions by the EDPA, and other applicable laws.

Mandatory Registration of DPO with EDPA

(17) The Data Controller or Data Processor shall register their DPOs with the EDPA.

Amendment of Guideline

(18) The EDPA reserves the right to amend the Guideline from time to time.