[*Company Logo*]

|  |
| --- |
| DATA PROTECTION OFFICER (DPO) JOB DESCRIPTION |

**DOCUMENT CONTROL**

|  |  |
| --- | --- |
| **Version:** |  |
| **Date of version:** |  |
| **Document Author:** |  |
| **Approved by:** |  |
| **Document Owner:** |  |

**REVISION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSION** | **REVISION DATE** | **REVISED BY** | **SUMMARY OF CHANGE/SECTION REVISED** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**JOB SPECIFICATION**

1. Advise [*Name of Company*] on compliance with applicable data protection legislation in Nigeria including but not limited to the Nigeria Data Protection Regulation (NDPR), the NITDA Act, the NDPR Data Protection Implementation Framework etc.
2. Liaise with the different functions of [*Name of Company*] that have responsibilities involving the processing of Personal Data of employees, vendors, clients and other Data Subjects including but not limited to– Human Resources, Sales and Marketing, Customer Service, Procurement, I.T.
3. The Data Protection Officer (DPO) shall be on the lookout for updates and changes to the provisions of relevant data protection legislation so as to effect these changes in the [*Name of Company*]’s policies and processes and also proffer accurate advice where necessary.
4. Work with the appointed Data Protection Compliance Organisation (DPCO) in ensuring that [*Name of Company*] duly complies with data protection legislation particularly in the timely filing of the Annual Data Protection Compliance Audit Report for [*Name of Company*] on or before the 15th of March every year (or other extended deadline).
5. Collaborate and coordinate relevant personnel of [*Name of Company*] in the event of a disaster which affects [*Name of Company*]’s systems and database so as to mitigate the effect of such disaster to the greatest extent possible. The DPO shall work with personnel from relevant departments including but not limited to IT, Human Resources to ensure the implementation of [*Name of Company*]’s security measures to address such disaster incident as may be provided in the [*Name of Company*]’s policies. Furthermore, the DPO shall ensure the communication of such breach/disaster incident to the regulatory authority and to the Data Subjects where such is deemed necessary.
6. Perform regular reviews of [*Name of Company*]’s internal policies to ensure that [*Name of Company*]’s processes and policies are in compliance with the provisions of the NDPR and other applicable data protection legislation.
7. Ensure [*Name of Company*]’s Management and Board of Directors are aware and consistently updated on the compliance requirements of the NDPR and related legislation and are compliant to the greatest extent possible.
8. Ensure that compliance risks such as potential fines are included into the Corporate Risk Register of the [*Name of Company*].[[1]](#footnote-1)
9. Ensure [*Name of Company*]’s contracts with its employees, clients, customers, vendors are regularly revised to include data protection clauses and general compliance with applicable data protection legislation.
10. Develop and improve all appropriate policies with data protection clauses such as HR Policy, Information Security Policy, Incident Management Policy, Privacy Policy, Data Breach Management Policy, Data Retention Policy, Disaster Recovery Policy, Data Protection Impact Assessment Policy etc.
11. Provide adequate support to process owners in conducting Data Protection Compliance Audits (DPCAs) and Data Protection Impact Assessments (DPIAs) in accordance with extant laws and relevant policies.
12. The DPO shall assist [*Name of Company*] in ensuring that there are adequate security measures in place to protect personal data and also ensure that [*Name of Company*]’s Information Systems are guided by an Information Security Standard. The DPO shall also lookout for updates in security standards so as to ensure that same are implemented in [*Name of Company*]’s security systems.
13. Provide adequate advice to [*Name of Company*] as regards the transfer of Personal Data to a foreign country and shall ensure that such transfer is done in accordance with the provisions of the NDPR.
14. Conduct regular capacity building for personnel of [*Name of Company*] to ensure compliance with the NDPR.
15. Ensure that the [*Name of Company*] has appropriate legal bases for all processing activities that it conducts on Personal Data at every point in time.
16. Ensure that the rights of Data Subjects to their Personal Data being processed by the [*Name of Company*] is safeguarded, protected and can be exercised in accordance with the provisions of the NDPR.
17. Act as [*Name of Company*]’s representative with the relevant DPCO as well as with NITDA.

**QUALIFICATIONS AND SKILLS**

1. Must have adequate knowledge and experience in Data Protection, Cybersecurity and Privacy functions.
2. Certification in Data Protection, Cybersecurity and Privacy Rights will be an advantage.
3. Client relationship skills to continuously coordinate privacy with Data Controllers, Administrators and third parties.
4. Relevant industry experience in privacy risk assessment and attainment of information security standards certifications.
5. Team coordination skills.

1. In addition to criminal liability, where a defaulter Data Controller deals with more than 10,000 Data Subjects, fine of 2% Annual Gross Revenue or 10 Million naira, whichever is greater. Where a defaulter Data Controller deals with less than 10,000 Data Subjects, fine of 1% of the Annual Gross Revenue or 2 Million Naira, whichever is greater. [↑](#footnote-ref-1)