[*Company Logo*]

|  |
| --- |
| NDPR COMPLIANCE CHECKLIST |

**DOCUMENT CONTROL**

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

**REVISION HISTORY**

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

|  |  |  |
| --- | --- | --- |
| SN | AREA OF COMPLIANCE | ACTION POINT |
| 1. | Governance | * Ensuring C-Suite Management and the Board of Directors are aware of the compliance requirements of the NDPR * Constant update of C-Suite; Management and the Board of Directors on NDPR Compliance; * Ensuring independence of DPO and direct access to C-Suite Management; |
| 2. | Risk Management | * NDPR risk in terms of potential fines should be part of the corporate risk register;[[1]](#footnote-1) |
| 3. | Audit Filing | * Data Controllers are to file their Annual Data Protection Audit Reports through a DPCO on or before the 15th of March of the following year. |
| 4. | Contract Documentation | * The Company’s contracts with its employees, clients, customers, vendors should be revised regularly to provide for data protection clauses and general compliance with data protection legislation. |
| 5. | Policy Documentation | * The DPO is to carry out regular reviews of the Company’s internal policies to ensure compliance with data protection regulations. * The DPO is to ensure that the Company has in place appropriate policies such as – HR Policy, Information Security Policy, Incident management policy, Privacy Policy, Data Breach Management Policy, Data Retention Policy, Disaster Recover Policy, Data Protection Impact Assessment Policy. |
| 6. | Advisory | * The Data Protection Officer is to advice the Company generally on compliance with relevant Data Protection legislation. Specifically, the DPO is to liaise with the following functions that have responsibilities for Personal Data: Human Resources, Sales and Marketing, Customer Service, Procurement, IT etc. * The DPO should be on the lookout for updates and changes to the provisions of data protection regulations so as to effect those changes in the Company’s policies and processes and proffer accurate advice where necessary. * The DPO should provide support to the process owner in the conduct of DPIAs. |
| 7. | Security | * The Company should have adequate security measures in place and also ensure that the Company’s Information systems are guided by an information security standard. * Measures such as encryption, anonymization and pseudonymization should be incorporated into the Company’s systems. These should also be included in the Company’s Information Security Policy. * The DPO should be on the look out for updates in security standards so as to implement same in the Company’s security systems. |
| 8. | Transfer to a foreign country | * Does the company transfer Personal Data outside Nigeria? * Is the receiving country on NITDA’s Whitelist? * If no, obtain consent of Data Subject or Adequacy Decision of NITDA. |
| 9. | Training and Awareness | * The DPO should ensure regular capacity building for himself as well as for other personnel of the Company to ensure compliance with the NDPR |
| 10. | Consent of the Data Subject | * Specific purpose of collection must be disclosed to Data Subject. * Consent must be obtained without fraud, coercion or undue influence. * Where consent is given in the context of a written declaration which also has details on other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters. * Language requesting consent must be plain and clear. * Prior to giving consent, data subject must be informed of his right and the ease to withdraw consent at any time. |
| 11. | Data Subject Rights | Ensure the Data Subjects Rights are protected and can be exercised in accordance with the provisions of the NDPR. The rights of the Data Subject under the NDPR include:   * Right to be informed * Right of consent * Right of access to Personal Data * Right to be forgotten * Right to Personal Data Portability * Right to restrict processing * Right to object * Right to rectification of Personal Data |
| 12. | Legal basis for processing data | Ensure that the Data Controller processes Personal Data on any of the following legal bases:   * Legitimate Interest * Legal Obligation * Public Interest * Contract * Vital Interest * Consent |

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)