Data Protection Policy

Preamble

In line with the Preamble of the Nigerian data protection policy (The National Information Technology Development Agency (NITDA)) mandated by the NITDA Act of 2007 to, inter Alia: develop regulations for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour and other fields, where the use of electronic communication may improve the exchange of data and information;

DOCUMENT CONTROL INFORMATION			
Document type	POL (Policy)	**Full Document Number**	OPEPOL001
Version:	1.0	**Superseded Version:**	
Originator:	Kushim Jonathan Agwom	**Job title:**	Data Manager
Department / Function:	OPE (Strategic Operations)	**Subject category:**	Data Protection
Authorship date:	8 – March 2022	**Published date:**	
Management Committee sign off date:		**Date for Review:**	

Please ensure you are viewing the current version of the document.

Target Audience	
People who need a detailed knowledge of the document	All staff involved in processing personal data
People who need a broad understanding of the document	
People who need to know that the Code of Practice exists	All staff, Volunteers and ZRC Project students

Contents

Introduction and Context

ZRC needs to process certain types of information about the people with whom it deals. This includes information relating to its staff, Project and IT students, Volunteers, and other individuals. It needs to process 'personal data' for a variety of reasons, such as to recruit and pay its staff, and to comply with statutory obligations (for example, health & safety requirements of its Staff).

The legislative framework for this is the ECOWAS Data Protection Regulation (GDPR) within ECOWAS "Supplementary Act A/SA. 1/101/10" as applied in the Nigerian Data Protection Regulation 2019. This policy outlines the responsibilities of staff, students and other parties connected with ZRC in ensuring compliance with this Regulation.

As required by Article 7 of the Regulation, ZRC is designated as a "Private authority" under the ECOWAS Data Protection Act "the Act" and is required to appoint a Data Protection Officer1.

ZRC acknowledges its obligations under the Regulation and is committed to protecting the rights and freedoms of all individuals whose personal data is processed as part of its business and research processes.

Equality and Diversity

ZRC is committed to promoting equality of opportunity, combatting unlawful discrimination, and promoting good community relations. We will not tolerate any form of unlawful discrimination or behaviour that undermines this commitment and is contrary to our equality policy.

Safeguarding

In line with our Safeguarding policy and procedures, ZRC's processes reflect our organizational commitment to keeping children and vulnerable adults safe.

OBJECTIVES OF THE REGULATION

The objectives of this Regulation are as follows:

1. to safeguard the rights of natural persons to data privacy.
2. to foster safe conduct for transactions involving the exchange of Personal Data.
3. to prevent manipulation of Personal Data; and
4. to ensure that Nigerian businesses remain competitive in international trade through the safe-guards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice.

SCOPE OF THE REGULATION

1. this Regulation applies to all transactions intended for the processing of Personal Data, to the processing of Personal Data notwithstanding how the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria.
2. this Regulation applies to natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria.
3. this Regulation shall not operate to deny any Nigerian or any natural person the privacy rights he is entitled to under any law, regulation, policy, contract for the time being in force in Nigeria or in any foreign jurisdiction.

DEFINITIONS

In this Regulation, unless the context otherwise requires:

1. “Computer” means Information Technology systems and devices, networked or not.
2. ‘Consent’ of the Data Subject means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.
3. “Data” means characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device.
4. “Database” means a collection of data organized in a manner that allows access, retrieval, deletion, and processing of that data; it includes but not limited to structured, unstructured, cached and file system type databases.
5. “Data Administrator “means a person or an organization that processes data
6. “Data Controller” means a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for, and the way Personal Data is processed or is to be processed.
7. “Database Management System” means a software that allows a computer to create a database; add, change, or delete data in the database; allows data in the database to be processed, sorted, or retrieved.
8. “Data Portability” means the ability for data to be transferred easily from one IT system or computer to another through a safe and secured means in a standard format.
9. “Data Protection Compliance Organization (DPCO)” means any entity duly licensed by NITDA for the purpose of training, auditing, consulting, and rendering services and products for the purpose

of compliance with this Regulation or any foreign Data Protection Law or Regulation having effect in Nigeria.

10. “Data Subject” means any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.
11. “Data Subject Access Request” means the mechanism for an individual to request a copy of their data under a formal process which may include payment of a fee.
12. “Filing system” means any structured set of Personal Data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.
13. “Foreign Country” means other sovereign states, autonomous or semi- autonomous territories within the international community.
14. “Regulation” means this Regulation and its subsequent amendments, and where circumstance requires it shall also mean any other Regulations on the processing of information relating to identifiable individual’s, including the obtaining, holding, use or disclosure of such information to protect such information from inappropriate access, use, or disclosure.
15. “Personal Data” means any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others;

16. “Personal Identifiable Information (PII)” means information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context
17. “Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, either by automated means or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
18. “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.
19. “Recipient” means a natural or legal person, public authority who accepts data.
20. “Relevant Authorities” means The National Information Technology Development Agency (NITDA) or any other statutory body or establishment having government’s mandate to deal solely or partly with matters relating to Personal Data.
21. “Sensitive Personal Data” means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.
22. “The Agency” means the National Information Technology Development Agency.
23. “Third Party” means any natural or legal person, public authority, establishment or any other body other than the Data Subject, the Data Controller, the Data Administrator and the persons who are engaged by the Data Controller or the Data Administrator to process Personal Data.

Roles and Responsibilities

1. The ZRC Board is ultimately responsible for ZRC's compliance with the Regulation via the ZRC Director and senior management team, with day-to-day responsibility delegated to the Data Protection Officer.
2. The Governance Oversight Committee is responsible for oversight of information governance at ZRC including data protection matters which includes reviewing and approving policies and related guidelines.
3. The Data Protection Officer has the following responsibilities:
    i. To inform and advise ZRC management and staff about their obligations under the Regulation.
    ii. To monitor compliance with the Regulation, the ZRC data protection policies and associated framework.
    iii. To provide advice where requested regards the data protection impact assessment and monitor its performance.
    iv. To cooperate with the Information Commissioner's Office (ICO);
    v. To act as the contact point for the ICO on issues relating to processing, including "prior consultation" as outlined in Article 36 of the Regulation.
    vi. Staff and students with responsibilities for processing personal data will adhere to the Policy and adhere to any other guidance or procedures accompanying it.
    vii. Staff and students will undertake training at least every two years (annual for those involved in high risk work), be aware of this Policy's existence, and seek advice and clarification on data protection matters from the Data Protection Officer.

General Data Protection Regulation (GDPR) principles

In respect to Part 2 of the Nigerian Data Protection Policies and Chapter V of ECOWAS Data regulation Polices

1. ZRC staff should be aware of the principles of the Regulation and ensure that these are addressed when dealing with personal data.
2. The first principle is legality, transparency, and fairness:
    i) For processing to meet the first principle you need to identify a lawful basis.

    This can include consent, but where this is the case the individual may have greater rights as a result, e.g. to have their data deleted. ZRC will always identify that legal basis and communicate this to a data subject before processing their data. Apart from consent, other possible legal bases are:

    - necessary for performance of a contract.
    - compliance with a legal obligation.
    - to protect the vital interests of the data subject or another person.
    - for the purposes of legitimate interests or in the exercise of official authority invested in the data controller.

    ii) For special categories of data, explicit consent is usually required
3. The second principle is purpose limitation:
    i) Personal data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.
4. The third principle is minimization:
    i) Processing of personal data should be adequate, relevant, and limited to what is necessary in

relation to the purposes for which they are processed.

5. The fourth principle is accuracy:
    i) Processing of personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.
6. The fifth principle is storage limitation:
    i) Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
7. The sixth principle is integrity and confidentiality:
    i) Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.
8. The final requirement of the controller, or “seventh principle” is accountability:
    i) Article 5(2) requires that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.” This is sometimes referred to as the “Seventh principle”. In practice, sufficient records and documentation need to be retained to demonstrate adequacy in this area.
9. In addition, the Regulation imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organizations; to ensure that the level of

protection of individuals afforded by the GDPR is not undermined. See the "Guidance Note for International Transfers of Personal Data" for further information.

Prohibited activities

The following activities are strictly prohibited:

1. Using data obtained for one purpose for another supplemental purpose (e.g. using personal data obtained from student registration for marketing purposes unless consent was obtained for this in the first instance);
2. Disclosing personal data to a third person outside of ZRC without the consent of the data subject.
3. Carriage of personal data on non-ZRC laptops or other devices which are not encrypted to standards set by IT Services.
4. If you have doubts about an activity not listed above, then please seek advice from the Data Protection Officer.

Subject access requests

In the with part three of the Nigerian Data Protection on the rights of the data subject

1. under the GDBR has the right to;
    i. Confirmation that their data is being processed.
    ii. Access to their personal data.
    iii. Other supplementary information (this mirrors the information provided in the privacy notice i.e. purpose of processing, categories of data being processed etc.
2. This right of access was referred to as a "subject access request" under the Data Protection Act 1998. The GDPR has reduced the response time from forty days to one month, and no fee can be charged. Such a request for access must be handled according to the "Subject Access Request

Procedure".

3. Third party access – this could be a party acting on behalf of the data subject. This may be allowed, but the appropriate procedures must be followed in ascertaining the right of the third party to make the request.
4. Freedom of Information requests for the requester's personal data. Any such request which is received by ZRC relating to the requester's personal data should be treated as a SAR.
5. When an SAR involves third party information you need to seek the other individuals' consent.
6. Exemptions may be allowed to SARs in certain circumstances which include the prevention of crime and assessment of taxes (see below). These exemptions apply where the release of the information is "likely to prejudice" the function of the organization to which the request is made. The advice given by the ICO is that this must constitute a "substantial chance" and not a mere risk that complying with the SAR would noticeably damage the discharge of the function concerned.

Release for crime and taxation

1. The legislation includes exemptions for the following purposes:
    i. The prevention or detection of crime.
    ii. The capture or prosecution of offenders; and
    iii. The assessment or collection of tax or duty.
2. However, the exemption applies, only to the extent that complying with a SAR would be likely to prejudice the crime and taxation purposes set out above.
3. A set of procedures exist which must be invoked in the event of an approach by an enforcement agency (e.g. Police, UK Border Force). The member of staff receiving the request must immediately

invoke these procedures and the release of information can only be authorized by the senior members of ZRC staff named therein.

Research data

1. ZRC staff embarking on research which involves personal data should ensure that they have understood this policy and associated guidance and have documented (as per privacy by design guidance) how they will comply. This includes completing a Data Protection Impact Assessment.
2. Personal data obtained or used for research should be limited to the minimum amount which is reasonably required to achieve the designed academic objectives. Anonymization techniques should be applied where possible so that the data subjects cannot be identified.
3. There are some exemptions in the legislation regarding data obtained for "…archiving, research, and statistical purposes", for example, allowing personal data to be held for longer than the original purpose it was obtained.

International transfers

1. Personal data can only be transferred outside the Nigeria in compliance with the conditions for transfer set out in Chapter 2 of the Regulation. The "exceptions in respect of transfer to a foreign country" outlines how transfers can be made in accordance with the Regulation.
2. ZRC undertakes to only transfer personal data where the organization receiving the personal data has provided adequate safeguards. These include legally binding agreements between public authorities or bodies and standard data protection clauses. Detailed information about this can be found in the https://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf and https://www.dataguidance.com/notes/nigeria-data-protection-overview

Risks And Implications of Breaching This Policy

1. A serious contravention of data protection legislation which breaches the rights of a data subject can lead to fines of up to 20 million Euros (or 4% of annual global turnover) whichever is the greater, and possible litigation against the individual or individuals responsible for the breach. Apart from the fine, such a contravention would be seriously damage to ZRC's reputation which, in turn, could have negative impact on relationships with our funders and regulatory authorities. As a result, ZRC takes its responsibilities very seriously and expects its staff and students to comply with this policy, and the training and guidance which has been provided.
2. Breaches of this policy by staff will be investigated, and where appropriate, formal disciplinary action may be taken up to and including dismissal.
3. Breaches of this policy by students will be investigated, and where appropriate, formal disciplinary action may be taken up to, and including termination of studies.