Data Privacy Policy

Version 1.0

	Document Control #:	1.0	Revision #:	
	Issue Date:	31-10-2023	Revision Date:	

	Originated By:	Reviewed By:	Approved By:
Sign.			
Name	Abdul Aziz Dajooh	Ishrat Ullah Khan	Mohammed Al Gadhi
Designation	Cyber Security Specialist	Senior Cyber Security Governance Specialist	Chief Executive Officer (CEO)

Document History

Release No.	Issue Date	Page No.	Line No.	Author	Changes
Ver 1.0	31-10-2023	N/A	N/A	N/A	N/A

Table of Contents

Abbreviations

Abbreviation	Description
ACIG	Allied Cooperate Insurance Group
PII	Personally Identifiable Information
NCA	National Cybersecurity Authority
IP	Internet Protocol
ID	Identity

1. Introduction

1.1 Purpose

This policy directive describes the measures taken by ACIG to protect the privacy of its employees and beneficiaries' (data subject) Personally Identifiable Information (PII).

1.2 Scope

This policy is applicable to all ACIG's systems, equipment, staff, and third parties who are employed by ACIG whether directly or indirectly.

1.3 Key Terms

Term	Description
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 (including ACIG employees and beneficiaries).
PII	Any information relating to an identified natural living person or to a natural living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, ID number, location data, IP address or other online identifiers or to one or more other factors specific to the person's identity.
Processing	Any operation or set of operations performed on PII or on sets of PII, whether or not by automated means, 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.
Controller	ACIG employee that determines the purposes and means of the processing of PII.

1.4 Roles and Responsibilities

Data and Chief Information Security officer/Date Protection Officer shall:

- Oversee policy compliance, violations, exceptions, and dispute resolution.
- Ensure alignment between this policy, ACIG's business, and strategy.
- Manage policy exceptions and violations.

The legal department shall:

- Define applicable privacy laws and regulations on ACIG;
- Execute their part in privacy impact analysis;
- Define privacy requirements in third parties' contracts or related documents.

Data Owners/heads of departments shall:

- Apply the requirements in this policy on the PII in their possession and demonstrate compliance.
- ACIG's users shall adhere to this policy and report any security incident or non-adherence to this policy to the Data and Cybersecurity Executive Director/ Data Asset Owners/Head of department.

1.5 Approval, Communication and Review

The Data privacy policy defined in this document shall be approved in accordance with the policy approval process of ACIG. After approval, these shall be published and communicated to all users. The set of data privacy policy shall be reviewed annually or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

1.6 Policy Relation

Section Name	NCA-ECC	ISO 27001	GDPR	NDMO-NDGP	NIST
Data and Information Privacy	2-7-3-3	A.18.1.4	Article 5 to 46	Section 5	Appendix J

2. Policy

2.1 General Policy Statements

- ACIG shall determine and documents applicable privacy laws and regulations. Also, ACIG shall monitor any changes or updates regarding the applicable privacy law and regulations to reflect it on its privacy policy, notice and practices.
- Unless it is necessary for a valid reason in the Saudi Law, explicit consent shall be obtained from a data subject to collect and process their data.
- PII shall be processed lawfully, fairly, and transparently concerning the data subject.
- Data privacy controls and mechanisms shall be implemented and enforced including pseudonymization, encryption, masking, and tokenization.
- Data privacy control mechanism should be (including and not limited to); as the technical choice of protection will be assessed by ACIG data and cybersecurity department.

2.2 ACIG PII Sources:

- Direct from data Subject with his/her consent.
- Indirect, and ACIG shall inform data subject within one month.
- Data Subjects' PII shall be protected (during its identification, Transferring, processing and destruction).
- ACIG shall determine, documents, and approve PII inventory for which PII is collected, used, processed, and shared, (if there was no purpose there should not be any collection for PII) that Illustrate:
  - The category of needed PII
  - Business needs and the purpose(s) for each PII category
  - PII retention time
  - The recipients or categories of recipients to whom the personal data have been or will be disclosed
  - PII source details if PII were not collected from the data subject directly,
- Data Subjects' PII shall be stored, processed, or transmitted in a manner that is accurate, adequate, relevant, and limited to what is necessary and according to business needs and PII retention that was defined in the data subject's consent and privacy notice.
- PII shall not be used for testing, training, or research Purposes.
- Data Subjects' PII shall be regularly reviewed and deleted based on business needs or PII retention that was defined in the data subject's consent and privacy notice.
- Periodic data privacy assessments of PII shall be performed.
- Data shall be hosted as per NCA regulations to be within Saudi Arabia. Within ACIG servers, or other entities related to ACIG.
- PII relating to criminal convictions and offenses, or related security measures shall be processed only under the control of official authority.
- ACIG shall store and process PII only inside the Kingdom of Saudi Arabia and enforce that in third-party contracts or related documents, and when ACIG needs to share PII with another entity outside the kingdom it shall seek National Data Management office approval.

2.3 Protection of PII

- ACIG shall ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- ACIG shall ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- ACIG shall regularly test, assess, and evaluate the effectiveness of technical and organizational measures for ensuring the security of the processing.
- PII shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- PII shall be accurate, appropriate, and kept up to date. Reasonable steps shall be taken to ensure that inaccurate PII concerning the purposes is erased or rectified without delay.
- PII shall be kept in a form which permits the identification of data subjects for the time necessary for the purposes of processing PII.
- Appropriate security controls shall be implemented to protect PII against unauthorized or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organizational measures.
- If PII is obtained from sources other than the data subject, the data subject shall be informed and ACIG Privacy notice should be sent to him/her too.

2.4 Data Subject Rights

- Where a data subject exercises a right under applicable privacy law, ACIG shall respond by taking any action required by the relevant privacy law, unless the request is obviously unfounded or excessive. ACIG shall take the relevant action within one month of receipt unless a different period is set by applicable privacy law. This applies to:
  - Right to get his/her authorization for collection, use, maintaining, and sharing of (PII) prior to its collection; OR prior to any new uses or disclosure of previously collected PII.
  - Right to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.
  - Right to withdraw his/her consent at any time.
  - Right to Access or get a copy of PII
  - Right to Rectification
  - Right to Erasure (Right to be forgotten)
  - Right to Restrict Data Processing
  - Right to be Notified
  - Right to Data Portability
  - Right to Object
  - Right to respond to his/her complaints, concerns, or questions.
  - Right to lodge a complaint with a supervisory authority.
  - Right to access ACIG Privacy notice.
  - Right to access all information in PII inventory.

2.5 Data Owner Rights

- Data owners should be informed of their rights, including the right to provide explicit or implicit consent for the collection, use, and disclosure of their personal data.

- Data owners shall have multiple options to grant or withhold consent for the collection, use, and disclosure of their personal data.
- Consent options should include both explicit and implicit consent mechanisms, allowing data owners to choose the level of consent that best suits their preferences and privacy concerns.
- Consent records should include details of the notification provided, the options presented to data owners, and the specific consent granted or denied by each individual.
- Data owners should be given the opportunity to review and verify the accuracy and completeness of their personal data before providing consent.

2.6 Privacy by Design

- ACIG shall adopt the principle of privacy by design and shall ensure that privacy requirements are satisfied on current, new, or significantly changed systems that collect or process PII.
- ACIG shall regularly conduct a privacy impact assessment on all systems that collect or process PII. This assessment shall include the following:
  - Applying PII Protection Principles
  - Fulfilling controller responsibilities
  - Implementing security controls to protect PII
  - Ensuring the legal basis for the processing of PII is clear and unambiguous
  - Ensuring that all staff involved in handling PII understand their responsibilities
  - Ensuring that PII are collected, used, processed, stored or shared for the authorized purpose(s) that identified in the privacy notices
  - Ensuring that ACIG provides effective notice to the public and to data subjects regarding any changes in its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII
  - Following the rules regarding the consent
  - Performing regular reviews of procedures involving PII
  - Adopting privacy by design for all new or changed systems and processes
- ACIG shall apply suitable data pseudonymization/anonymization techniques and encryption to protect PII.
- ACIG shall satisfy the following documentation requirements and make accessible by data subjects regarding its processing activities on PII:
  - Purposes of PII processing
  - Processing activities conducted on PII
  - Categories of PII processed
  - Agreements and mechanisms for the transfer of PII from and to other organizations after getting data subject consent or request
  - PII retention schedules
  - Security controls in place to protect PII
- ACIG's employees shall be made aware of this policy and their role in protecting PII.

2.7 Privacy by Default

- ACIG shall put in place appropriate technical and organizational measures for ensuring that, by default, PII is not processed unnecessarily. This applies to the amount of PII collected, the extent to which it is processed, how long it is stored, and who can access it. ACIG shall ensure that, by default, PII is not made available to an indefinite number of people without some action by the data subject.

2.8 Transfer of PII

- Any transfer of PII should be based on data subject consent or request.
- Before the transfer of PII outside ACIG, privacy impact analysis should be implemented.
- A proper notice should be sent to data subject including recipients to whom the PII will be transferred, including the Date, nature, and purpose of each disclosure of a record; and the names and addresses of the recipients to which the disclosure was made.
- The adequacy of the protection of PII at the receiving end shall be confirmed; this includes:
  - Receiving organization name and relevant details
  - Purposes of PII processing
  - Categories of individuals and PII processed
  - Categories of PII recipients
  - Agreements and mechanisms for transfers of PII
  - PII retention schedules
  - Relevant technical and organizational controls in place

2.9 Requirements for Third Parties

- ACIG shall establish, document, and approve privacy requirements (collection, use, processing, and sharing) for contractors, processors, and service providers; and include it in contracts and other related documents.
- Where ACIG and another controller jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under applicable privacy laws and regulations.
- Where processing is to be carried out on behalf of ACIG shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of applicable privacy laws and regulations and ensure the protection of the rights of the data subject.

2.10 Processing records and monitoring

- ACIG shall record the processing activities. That record shall contain but not limited to the following information:
  - The name and contact details of the controller and processer
  - The purposes of the processing
  - A description of the categories of data subjects and of the categories of personal data
- ACIG shall make the record available to the organization auditor and supervisory authority on request.
- ACIG shall regularly review PII inventory to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

2.11 Privacy Notice

- ACIG shall determines, document, approve, and implement requirements to provides effective notice to the public and data subjects regarding:
  - Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII
  - Authority for collecting PII

- The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices
- The right to access and have PII amended or corrected if necessary
- The PII the organization collects and the purpose(s) for which it collects that information
- How the organization uses PII
- Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing;
- Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent;
- How individuals may obtain access or get PII;
- How the PII will be protected;
- The period for which the PII will be stored
- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- The existence of the right to withdraw consent at any time,
- The right to lodge a complaint, concerns, or questions to ACIG and to lodge a complaint with a supervisory authority
- Whether the provision of personal data is legally required, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- The changes in practices or policies that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change

- ACIG shall ensure that its privacy practices are publicly available through organizational websites.
- ACIG shall inform the data subject before the restriction of processing is lifted. If processing was restricted by the data subject, personal data shall, with the exception of storage, only be processed with the data subject's consent.
- ACIG shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data has been disclosed. The controller shall inform the data subject about those recipients if the data subject requests it.
- ACIG shall inform data subject of the appropriate safeguards of transferring where personal data are transferred to a third country or to an international organization.
- ACIG shall ensure that the public has access to information about the identity and the contact details of the organization.
- Personal data breach shall notify within the time frame specified by the National Data Management Office's policy on personal data protection, which is 72 hours from the time the breach is discovered.
- ACIG shall ensure that the public has access to information about its privacy activities and is able to communicate with its Privacy Officer.
- ACIG shall ensure that its privacy practices are publicly available through organizational websites.

2.12 Privacy Breach

- ACIG shall develop, document, and approve a Privacy Incident Response Plan and implement it when needed.

- ACIG If a breach has occurred with a probability to result in a risk to the privacy or protection of PII, then ACIG following Privacy Incident Response Plan Procedures shall inform the DCS department within 72 hours.
- ACIG shall develop, document, approve, and implement a procedure to communicate the PII breach to the data subject without delay.

2.13 Training and Awareness

- ACIG shall develop, document, approve, implement, and update Regularly a comprehensive training and awareness program aimed at ensuring that personnel understand privacy responsibilities and procedures, such as administering basic privacy training and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII.