GSIS Government Service Insurance System
Financial Center, Pasay City, Metro Manila 1308

POLICY AND PROCEDURAL GUIDELINES NO. 373-21

FUNCTIONAL AREA : Data Privacy

DISTRIBUTION : The Board of Trustees
The President and General Manager
The Corporate Secretary
The Executive Vice Presidents
The Senior Vice Presidents
All Vice Presidents
All Department and Branch Managers
All Committee Chairpersons

SUBJECT : **MANAGEMENT OF DATA BREACH AND SECURITY INCIDENTS RELATIVE TO DATA PRIVACY AND PROTECTION**

I. Background/Rationale

To effectively implement the Data Privacy Act (DPA) and to give guidance in managing data breach and security incidents, the National Privacy Commission (NPC) issued NPC Circular 16-03, requiring any natural or juridical person in the government or private sector processing personal data or Personal Identifiable Information (PII) to promptly notify the NPC and the affected Data Subjects relative to the data breaches and security incidents.

This PPG is being issued to provide guidelines on handling of breach and security incidents, in compliance with Republic Act (RA) No. 10173, otherwise known as the DPA of 2012 and its Implementing Rules and Regulations (IRR)[1] and NPC Circular 16-03 for Personal Data Breach Management.

II. Objectives

This PPG aims to:

1. Provide standard process in the management, reporting, notification and resolution of Data Breach and Security Incident;

2. Identify individuals and groups directly involved in the processing, security and protection of Personal Information; and

3. Establish controls and measures to prevent or minimize the occurrence of Data Breach and Security Incidents.

[1] *Circulated on 24 August 2016 by NPC*

III. Definition of Terms

Application System User	Personnel who utilize computer systems in their daily tasks.
Data Protection Officer[2] (DPO)	An individual designated by the head of agency to be accountable for the agency's compliance with the DPA; Provided, that the individual must be an organic employee of the government agency; Provided, further, that a government agency may have more than one data protection officer.
Data Subject[3]	An individual whose personal, sensitive personal, or privileged information is processed.
Encryption	The process of converting information or data into a code, especially to prevent unauthorized access.
Filing System[3]	Any act of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.
Juridical Person	Is a body of persons, a corporation, a partnership, or other legal entity that is recognized by law which grants a juridical personality separate and distinct from that of a shareholder, partner or member.
Partner/s	Any of a number of individuals with interests and investments in a business or enterprise, among whom expenses, profits, and losses are shared.
Personal Data[4]	All types of personal information. The use of the term personal data shall refer to both

[2] *Section 3 of Rule 1, NPC Circular 16-03*
[3] *Section 3, DPA of 2012*
[4] *Section 3, IRR- DPA of 2012*

	personal and sensitive personal information.
Personal Data Breach[5]	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. A Personal Data Breach may be in the nature of: 1. An availability breach resulting from loss, accidental or unlawful destruction of personal data; 2. Integrity breach resulting from alteration of personal data; and/or 3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.
Personal Information[6]	Any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
Personal Information Controller (PIC)[6]	A natural or juridical person or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes: 1. A natural or juridical person, or any other body that performs such functions as instructed by another person or organization; or 2. A natural person who processes personal data in connection with his or her personal, family, or household affairs. There is control if the natural or juridical person, or any other body, decides on what information is collected, or the purpose or

[5] *Section 3 of Rule 1, NPC Circular 16-03*
[6] *Section 3, IRR- DPA of 2012*

	extent of its processing.
Personal Information Processor (PIP)[7]	Any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a Data Subject.
Privacy Impact Assessment (PIA)[7]	Is a process undertaken and used by a government agency to evaluate and manage privacy impacts.
Personally Identifiable Information (PII)	Is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.
Process Owner	Is a person who is given the responsibility and authority for managing a particular process. Although portions of the process may be delegated, the process owner remains responsible for their monitoring.
Processing[8]	Refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modifications, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
Secure Sockets Layer (SSL)	A standard security technology which provides an encrypted link for securing information passed on between a browser/client and webserver/server.
Security Incident[8]	Is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. It includes incidents that would result to a Personal Data Breach, if not for safeguards that have been put in place.

[7] *Section 3 of Rule 1, NPC Circular 16-03*
[8] *Section 3, IRR- DPA of 2012*

Sensitive Personal Information[9]	Refers to personal information: 1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; 2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; 3. Issued by government agencies peculiar to an individual which includes, but not limited to social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and 4. Specifically established by an executive order or an act of Congress to be kept classified.
Transport Layer Security (TLS)	An encryption protocol that provides end-to-end security of data sent between applications over the internet.
Virtual Private Network (VPN)	An encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted.
Vulnerable Groups	Groups of individuals which often include children, ethnic groups/ minorities, persons with limited lifespan, persons suffering from dementia, persons with mental disorders, abusers of drugs and alcohol and persons with disabilities.

[9] *Section 3 of Rule 1, NPC Circular 16-03*

IV. Policies

A. Coverage

These guidelines shall cover any natural and juridical person in the government or private sector, all application users whether permanent or coterminous employees, job order personnel, consultants, contractors or third party users who has access to personal data within GSIS' information, communication and/or relevant filing systems.

All application system users whether permanent employees, co-terminus, job order personnel, consultants, contractors or third party users are required to be aware of, and follow these guidelines in the event of a Personal Data Breach.

Any personal data contained in any medium that is in the custody of GSIS is covered by these guidelines.

B. Data Breach Response Team (DBRT)

In compliance with the requirements of the Data Privacy Act or RA No. 10173, an Office Order on the Creation of DBRT was approved and implemented.

1. Composition of DBRT:

DBRT	:	Vice President, Information Security Office (ISO), Data Privacy Officer (DPO) and Chairperson, Data Privacy and Protection Committee
		Vice President, Risk Management Office (RMO)
		Vice President, Application Management Office (AMO)
		Vice President, Adjudication and Policy Office (APO)
		Vice President, Corporate Communication Office (CCO)
Ad Hoc Member/s to the DBRT	:	Vice President or Manager of concerned Office

2. Responsibilities of DBRT:

a. The DBRT shall manage possible violations in information security and data privacy in accordance with the Guidelines on the Creation of GSIS Data Privacy and Protection Committee (DPPC) including its amendment.

b. The DBRT shall evaluate the security incident, reduce and/or resolve consequential damage, restore trust of stakeholders and integrity of the information and communications system, and comply with reportorial requirements.

C. Measures to Prevent the Occurrence of Data Breach and Security Incidents

Every Personal Information Controller (PIC) and Personal Information Processor (PIP) shall consider the human aspect and technical requirements of data protection. In line with this, applicable organizational, physical, and technical security measures shall be implemented by GSIS, as the PIC, in order to prevent security breaches.

1. Organizational Measures

a. The GSIS Data Privacy and Protection Committee (GDPPC) shall ensure compliance by the GSIS with the DPA, its IRR, issuances by the National Privacy Commission (NPC), and other applicable laws and regulations relating to privacy and data protection.

b. The Information Security Office (ISO) shall head the implementation of security measures. Similarly, the GDPPC shall lead the resolution of data breach complaints and incidents.

c. The Vice President (VP), ISO, shall be the designated chairman of the GDPPC and the GSIS Data Protection Officer (DPO).

d. All the Managers in the Central Office and Branch Offices as well as the Extension Office Heads shall be designated as Data Compliance Officers (DCO). They shall be responsible in preparing and updating their own Privacy Impact Assessment (PIA), and, in reporting to the DPO any occurrence of data breach within their respective jurisdictions.

e. The Risk Management Office (RMO), in coordination with the process owners, shall lead the conduct of the Privacy Impact Assessment (PIA) at least every two years in relation to all existing systems, processes, and forms which include and/or contain personal data.

   On the other hand, PIA shall be performed on all new systems before being implemented, and at least every two (2) years thereafter.

f. The operating unit concerned (OUC) shall include in the submission to the Strategic Planning and Control Department (SPCD) of the Office for Strategy Management (OSM) the PIA for proposed programs and projects which involve personal information.

g. The DPO shall see to it that all data processing systems being used by the GSIS are registered with NPC as part of our compliance with DPA.

h. ISO shall perform an annual review of the roles and access levels of the end-users.

   The access granted to GSIS systems shall be on a need to know, need to have basis, and shall be compliant with the provisions of the Guidelines on Access Controls.

i. GSIS personnel involved in the processing of Personal Information shall be provided annually with trainings and seminars related to data breach and security to ensure that the policies on data privacy and security are consistently implemented and genuinely instilled in the processes of GSIS.

   Trainings and seminars shall be conducted twice a year by the GDPPC, in coordination with the Human Resources Office (HRO), to promote awareness and render the GSIS personnel updated on developments in data privacy and security.

j. The GDPPC in coordination with the CCO shall annually conduct an information awareness program or issue advisories regarding any updates issued by NPC.

k. The HRO shall require the execution of Non-Disclosure Agreement (NDA) by all employees, job-order (JO) personnel and on-the-job (OJT) trainees.

l. The procuring units shall ensure that data privacy compliance provisions are included in the contract or bid documents when securing services from third parties i.e., Security, Janitorial, Call Center, Text Blast, etc.

m. The NDA shall form part of the contract to be executed by the GSIS' service partners/providers and other third parties who will have access to the personal information of its employees, members and stakeholders.

n. The DPPC shall record and document activities that shall be carried out by the GSIS in order to ensure compliance with the DPA, its IRR, and other relevant issuances.

o. The guidelines relating to data privacy and protection shall be reviewed and enhanced annually, if needed, and shall be aligned with the principles of transparency, legitimate purpose and proportionality.

   The DPO or officer duly designated through an Office Order by the President and General Manager shall lead the review and updating of the said guidelines.

2. **Physical Measures**

a. The GSIS shall maintain the personal data of its stakeholders either in paper-based or physical and/or in digital or electronic format.

b. This information shall be stored in records rooms, vaults, filing cabinets, electronic data storage, and other back-up media and devices.

c. All physical storage containing personal information shall be locked when not in use and access shall be strictly limited to authorized personnel only.

d. Unneeded printed documents i.e., working papers, screen shots, misaligned or poor quality and photocopy of documents containing personal data shall not be used as scratch papers and shall, instead, be shredded. The shredded documents shall be turned-over to RMD, following the guidelines on the disposal of records and shall be included in the controlled disposal of documents.

e. All records rooms shall be provided with appropriate security measures in order to safeguard the availability, integrity, and confidentiality of records, particularly those containing Personal Data. Closed-Circuit Televisions (CCTVs) or surveillance cameras shall be installed in areas where physical and electronic data are being kept.

The installation of CCTVs should be in conformity with the existing guidelines on records management, security of vaults, safes, grill doors, steel cabinets, and records, storage and executives' rooms and administration of the internet protocol (IP) and CCTV system for Central and Branch Offices.

f. The Building and Maintenance Department (BMD) shall ensure the availability of sufficient number of fire extinguishers in all records rooms.

g. The data center, data recovery site, and backup media off-site storage shall be considered as highly restricted areas and shall be secured at all times.

Likewise, access to these areas shall be strictly controlled and monitored by the Data Center and Data Recovery Department, ITSG.

h. Entry to the above-mentioned facilities shall require a formal request and approval from either the Vice President – General Services Office for the records rooms or the Vice President – Information Technology Infrastructure Office for the electronic data-related areas.

Actual entry to the said facilities shall be logged accordingly.

i. The computers of GSIS personnel who process personal data shall be positioned with ample space from aisles or corridors so that the privacy of the information shown on screen will not be compromised or exposed to privacy risk.

   In a similar manner, the frontline personnel and those assisting the pensioners and e-card concerns shall have considerable spaces between them such that conversations remain private between the data subject and the GSIS personnel.

j. Before leaving the work area, employees shall ensure that his or her desk or work station is clear of documents that contain personal information. However, if not possible to remove the documents from their tables or work area, because of the volume and still working on them, secure the information by covering them with a blank paper or put the records face down.

k. The Information Technology Services Group (ITSG) shall implement, whenever necessary, the use of computer screen privacy filter of the computers of GSIS personnel who process personal data in order to protect them from accidental disclosure.

l. GSIS personnel who are involved in the processing of personal data shall not store these information on their personal gadgets.

m. The storage, retention, maintenance and disposal of GSIS documents and records shall be in accordance with existing policies on records management and based on the schedule stated in the GSIS Records Disposition Schedule (RDS).

3. **Technical Security Measures**

a. Transmission of data with personal information shall be protected by encryption technologies, such as VPN, SSL and or TLS, or be protected with a password by the Unit or personnel transmitting the data.

b. The ISO shall require the GSIS personnel involved in the processing of personal information to use data encryption, password protection, or any similar data protection technology to files containing personal data that are to be transmitted within the organization or to third parties.

c. Saving of member's personal information in USB, CDs or external drive, shall be avoided. However, if necessary, ensure that the media is encrypted to protect the information stored therein, in case of theft or loss.

d. Data retention shall be defined by the Information Asset or Data Owner to ensure that data on the servers or workstations are identified and comply with the retention requirement.

e. Information security monitoring systems, shall be utilized by ISO to protect or detect possible data security breaches and/or hacking attempts against GSIS.

f. In order to protect the security of the Personal Information in the custody of GSIS, the ISO shall perform an annual vulnerability scanning of computer systems and networks, including vulnerability and source code scanning on new systems prior to implementation.

g. The Information Security Policy shall govern the various security measures which shall be implemented within GSIS.

D. Management of Data Breach and Security Incident

1. Reporting of Security Incidents or Personal Data Breach

a. The individual who discovered any data breach or security incident shall report it within Three (3) hours to the DPO through e-mail or phone call, and by filling-out the Personal Data Security Breach Report Form (**Annex A**). The DPO, shall then, inform the DBRT upon receipt of the report.

This shall be simultaneously reported by the concerned individual to his or her superiors, Heads of Security Department, ISO, ITSG or Records Management Department (RMD), whichever is applicable.

b. The DBRT shall require the following from the GSIS personnel involved in a security incident or Personal Data Breach within Forty- Eight (48) hours from discovery of the incident:

1) Formal report to the Security Department if the incident happened within the Office premises;

2) Copy of formal complaint or blotter report to the barangay and police station at the location of the incident when it takes place outside the Office premises;

3) To notify the DPO and ITSG if database or digital file; DPO and RMD if physical file; and

4) Execution of affidavit, if applicable.

c. The DPO, together with the DBRT, shall evaluate and determine the necessity to report within the prescribed period of Seventy Two (72) hours any incident or breach to the Management Committee, the President and General Manager, Board of Trustees (BOT), NPC, and Data Subjects.

d. The DBRT shall determine the need to notify law enforcement or other investigative bodies within ten (10) working days upon discovery of the incident.

e. The reports of the DBRT shall include the description of the data breach or security incident, the root cause analysis (RCA), actions and decisions, notifications (**Annex B**), and the support provided to the Data Subject.

f. The DPO shall coordinate with NPC, and act as the focal point for matters pertaining to the processing of the data breach and security incidents.

2. Internal Assessment and Investigation

a. When a report on Data Breach has been received, an initial assessment shall be conducted by DPO and DBRT in order to evaluate and identify the nature and scope of the incident, its impact to the unit in charge of the data and to the GSIS, the severity level of the incident (**Annex C**), the persons and Data Subjects involved, the available evidence and the next steps to be taken.

b. An investigation shall be undertaken in order to completely appraise the extent of the breach. The DPO, together with the DBRT, shall discuss cases that would impact a specific group of Data Subject or those distinctive cases which do not fall under a general categorization, and shall come up with a resolution and/or recommendation.

c. The DPO shall assign a DBRT member to take charge in undertaking the investigation based on the nature of the incident.

3. Containment and Eradication of the Breach

a. The DPO and the DBRT shall provide assistance to the affected Data Subjects in order to secure or clear their Personal Information.

b. The DBRT, applying the severity matrix, shall outline the actions or measures to be taken or proposed to be taken including their descriptions to address the data breach or security incident, which shall be submitted to the DPO and the GSIS.

c. The DPO shall see to it that protection and security of Personal Information remains a priority, hence, continuous partnership with the Risk Management Office (RMO) shall be required to mitigate or prevent the recurrence of the incident. The Process Owner or the GDPPC, as the case may warrant, shall monitor and control the actions taken or to be taken to contain or eradicate the breach. RMO, in turn, shall ensure that mitigating and preventive measures are in place to prevent the recurrence of the incident.

4. Notification to NPC

a. The NPC shall be notified when the breached personal data:

1) Contain information that could affect national security, public safety, public order, or public health;

2) Correspond to at least one hundred (100) Data Subjects;

3) Must be kept confidential under applicable laws or rules; or

4) Belong to vulnerable groups.

b. The DPO shall notify NPC through the submission of a report to the Office of the National Privacy Commission or through an email to dpo.ace@privacy.gov.ph.

The DPO shall ensure that the incident is reported strictly within Seventy-Two (72) hours from determination of the breach. On the other hand, the full documentary report shall be provided to NPC within five (5) working days.

The DPO may request NPC for an extension to submit the full report when warranted.

c. The report shall include the following, but not limited to:

1) Description of the breach, Personal Data involved, and the loophole or negligence which caused the breach;

2) Chronology of events leading to the breach;

3) Name and contact details of the DPO and the GSIS;

4) Manner by which the Data Subjects will be notified and reasons for the delay in such notification, if warranted; and

5) Number of Data Subjects or records involved in the incident.

d. The DPO shall remain accountable for notifying NPC even if the breached data has been outsourced or subcontracted to an external PIP.

5. Notification to Data Subject

a. Notification of individual Data Subject shall be required when any of the following condition is met:

1) The Personal Data which can give rise to identity fraud is present in the data that has been breached;

2) The Personal Data may have been obtained by an unauthorized person; or

3) The unauthorized access to the Personal Data may cause risk or harm to the Data Subject.

b. The DBRT shall exert reasonable effort to ensure that notification is undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.

c. The DPO shall ensure that notification of the Data Subject is done in a secured channel, either by secured email or sent through mail courier requiring proof of delivery and signatory of the recipient. However, when resources of significant number or cost are required to inform the Data Subjects, the GSIS, through the President and General Manager (PGM) shall request NPC for approval in using alternative means of notification such as through public communication or any similarly effective means.

d. The DPO shall provide a medium for the affected Data Subjects to communicate with the GSIS in order to get clarifications or detailed information regarding the breach.

e. In the event NPC will require notification of Data Subjects, the GSIS, through the PGM, may request from NPC an exemption or deferment of the notification of Data Subjects.

6. Security, Recovery and Restoration of Personal Data

a. ITSG and ISO shall:

1) Develop a facility that will enable ISO to compare the compromised database against its back-up copy in order to ascertain any inconsistencies or modifications which could have resulted from the incident;

2) Put in place the required security controls such as, but not limited to, access control, back-up solutions, data encryption, and security log files;

3) Implement deletion and degaussing processes when disposing of equipment, storage device and back-up tape cartridges; and

4) Conduct monitoring for security breaches and vulnerability scanning of computer networks annually or whenever the need arises specifically when a security breach occurred.

b. Ensure the availability and confidentiality of the Personal Data which GSIS collects from its stakeholders;

c. Prioritize the integrity of the computer application systems and the databases; and

d. Review the policies and procedures on data breach management annually, including the testing, assessment, and evaluation of the effectiveness of the security measures.

7. Documentation of Data Breach Incidents

a. The GDPPC Secretariat shall keep an inventory log, both manual and electronic, of every incident or breach encountered, as well as an annual report, to be submitted to Management and to the NPC every 15th working day of the following year.

b. All actions of GSIS or its PIP in response to the incident shall be copy furnished the management.

c. The GDPPC, in coordination with RMO, shall conduct a PIA every two (2) years or whenever necessary, in order to identify the possible risks which may arise in the handling and processing of Personal Information.

The PIA shall be reviewed to make sure that such risks are identified, and minimized, if not totally eliminated.

d. All new GSIS systems and processes that will be collecting and processing personal data shall be subject to a privacy impact assessment to ensure that the said systems and processes observe the privacy principles.

e. The DPO shall initiate a PIA when a risk or vulnerability has been identified in any of the data processing activities. Similarly, an investigation to establish if a breach has occurred shall be undertaken.

f. The result of the PIA shall be applied to the affected processes or procedures to guarantee that adequate security controls are in place.

E. Security Measures

The Units shall ensure that the creation and collection, storage and transmittal, use and distribution, retention, as well as disposal and destruction of the personal data of members, pensioners and other stakeholders, as required by this PPG, adhere to the requirements of the DPA.

F. Penalties and Sanctions

The DBRT shall, upon assessment of the findings of the investigation, shall submit its recommendation to the Legal Services Group for further investigation and necessary legal action. The concerned employee may be held administratively, civilly and/or criminally liable, if warranted.

G. Reportorial Requirements

1. The Personal Data Security Breach Report Form (**Annex A**) shall be used when reporting a data breach or security incident.

2. The DPO shall:

    a. Report the following to Management Committee (ManCom) and the BOT:

        1) Occurrence of breach and other information security related incidents regardless of its severity; and

        2) Outcome of post-breach review including recommendations.

    b. Summary of breach monitoring and incident report to the ManCom, BOT, and to the NPC every 15th working day of the following year.

V. Procedures

The detailed procedures to be included in the Manual of Operations of the Operating Units Concerned (OUCs) shall adhere to the following general procedure/s:

Activity	Responsible Person/Unit
1. Receive data breach or incident report either through email, call and report from individual and or Unit who discovered the breach (**Annex A**).	DPO GDPPC Secretariat Concerned Superiors ISO Head of Security Department ITSG for electronic data RMD for paper-based data
2. Log incident report using Breach Log Report Template and forward to DBRT within the same day of its receipt. Indicate the following in the report: a. Date of incident/breach b. Name of person reporting the breach c. Contact details of the person reporting the breach d. Brief description of the incident/ breach e. Number of Data Subject affected f. Type of Data Subject g. Action Taken/Status	GDPPC Secretariat

Activity	Responsible Person/Unit
3. Issue Acknowledgment Receipt Form (**Annex D**) to confirm receipt of Personal Data Security Breach Report Form.	GDPPC Secretariat
4. Convene a meeting with the DPPC and DBRT to evaluate the breach. Determine the succeeding actions to be taken: a. If to be reported, prepare report. Proceed to Activity 6. b. If not, perform further investigation.	GDPPC
5. Validate required report and documents by using Severity Assessment Matrix for Data Breach (**Annex C**).	DBRT
6. Report incident or breach to the ManCom and BOT and request approval for the actions to be taken.	DPO
7. Coordinate with NPC regarding the incident and the action to be taken by GSIS, if necessary.	DPO
8. Prepare a notification letter for the data subject/s through postal or electronic mail if the former is not possible or if sending through eMail will prove to be cost beneficial to GSIS by using **Annex B**.	GDPPC
9. Provide assistance to affected Data Subjects to secure, recover or restore lost data.	DPO Process Owners
10. Monitor actions taken or to be taken.	DPO DBRT
11. File and log as closed and resolved.	GDPPC Secretariat
12. Conduct post-breach review and recommend actions to mitigate or prevent the recurrence of the incident.	GDPPC
13. Determine if PIA is warranted.	GDPPC
14. Report outcome of post-breach review including recommendations to ManCom.	DPO

Activity	Responsible Person/Unit
15. Prepare annual/summary report to the NPC.	DPO GDPPC Secretariat
16. Submit the report to NPC.	GDPPC Secretariat
End of Process	

VI. Data Privacy

The OUC shall ensure that the creation and collection, storage and transmittal, use and distribution, retention, as well as disposal and destruction of the personal and sensitive personal data of members, pensioners and other stakeholders, as required by this PPG, adhere to the requirements of the Data Privacy Act.

VII. Information Dissemination

The CCO shall prepare the information materials for the dissemination of this PPG.

The attached Memorandum Circular (**Annex E**) shall be issued by the GSIS to inform the public of this PPG.

VIII. Repealing Clause

All Office Orders, Circulars, Advisories, Policy and Procedural Guidelines which are inconsistent herewith are hereby superseded or modified accordingly.

IX. Effectivity Clause

This PPG shall take effect fifteen (15) calendar days from the date of publication in the Official Gazette or in a newspaper of general circulation.

ORIGINAL SIGNED
ROLANDO L. MACASAET
President and General Manager

Date Signed: AUG 24 2021

Document Control
Reference No.:_____
Issue No.: _____
Issue Date: _____

Republic of the Philippines
GOVERNMENT SERVICE INSURANCE SYSTEM
GSIS Building, Financial Center, Roxas Boulevard, Pasay City 1308

PERSONAL DATA SECURITY BREACH REPORT FORM

If you discover a Personal Data Security Breach, please notify your Head of Department immediately. Please complete this form and submit to the Data Protection Officer or to the Head Secretariat, GSIS Data Privacy Protection Committee (GDPPC) as soon as possible.

Notification of Data Security Breach		
Date	:	
Date incident/breach was discovered	:	
Name of person reporting the incident	:	
Contact details of the person reporting the incident	:	
Brief description of the Personal Data Security Breach (Who discovered the breach, what was stolen, how was it stolen, what systems were attacked, etc.)	:	
Number of data subjects affected (if known)	:	
Type of data subjects- members, pensioners, employees, others (if others, please specify)	:	
Brief description of any action taken since breach was discovered	:	
For GDPPC Use Only		
Report received by	:	
Date	:	
Action	:	
Date	:	

Republic of the Philippines
GOVERNMENT SERVICE INSURANCE SYSTEM
GSIS Building, Financial Center, Roxas Boulevard, Pasay City 1308

Date of Notice: _____

MEMBER/CLIENT NAME

Dear Sir/Mam:

At GSIS, we respect the privacy of our personal data. We are writing to let you know about a data security incident that involves the personal information you have with us.

On (date), we have discovered a data breach in our (systems). The data accessed may have included the following types of personal information:

- (Enumerate the types of personal information breach, e.g., First and Last Name, email, address, etc.)

To the best of our knowledge, the data accessed did not include any of the following:

- (Identify types of sensitive personal information not breached)

We deeply regret that this incident occurred. We have reported the incident to the National Privacy Commission (NPC) and (identify other government entities) which is/are currently conducting an investigation of the extent of the breach.

We, at GSIS has been reviewing the affected records, processes and all of our computer systems that may have impacted by the breach. Likewise, we, at GSIS have implemented the following measures to contain the breach:

- Identify the action taken

We will notify you if there are any significant developments.

Respectfully yours,

DATA PRIVACY OFFICER

Severity Assessment Matrix for Data Breach

The severity of a breach refers to the possible extent of consequence to a Data Subject that could ensue once his or her personal or sensitive personal information has been compromised.

An assessment matrix for a data breach must be established in order to have a standard quantitative tool that will guide the Data Protection Officer (DPO) and the Data Breach Response Team (DBRT) in assessing the severity of the breach, the actions to be taken, the notifications that must be sent out, and the mitigating measures that must be implemented.

In order to properly assess a breach, quantitative measures should be specified and should cover as much scenarios as possible. The DPO, together with the DBRT, must discuss cases that would impact a specific group of data subject or those very special cases which do not fall under a general categorization.

The following comprise the details necessary in assessing a data breach:

1. Type of data that was compromised. The type of data must be considered, whether they are simple personal information or sensitive personal information from which health conditions, financial state, and/or private preferences can be obtained. A higher assessment must be allotted to those cases that could give rise to losses, possible harm or humiliation to the data subject.

2. Ease of linking or identifying a data subject to the compromised data. The compromised data shall be evaluated whether it can be directly linked to the data subject or a certain degree of processing is required to ascertain the identity of a data subject. A lower assessment must be given to cases where processing, research or investigation is necessary before a compromised data can be linked to a certain data subject. On the other hand, a very high assessment must be provided to compromised data that could easily and readily be linked to a data subject.

3. Circumstances leading to the data breach and its consequences. The intent and the effect of the data breach must be carefully analysed. It has to be established if there is malicious intent to commit identity theft or fraud, to physically harm or humiliate and damage the reputation of a data subject or it is simply an accidental or unintentional loss of confidentiality, integrity and/or availability of data.

INCIDENT PRIORITY			SEVERITY			
			4 – LOW	3 – MED	2 – HIGH	1 – VERY HIGH
			• No significant impact on the Data Subject • No required action on the part of GSIS as well as the Data Subject.	• With significant inconvenience on the Data Subject • With minimal action on the part of GSIS as well as the Data Subject • With minor interruption of service to affected Data Subject • Possibly with need to notify Data Subject and report the breach to NPC	• With significant consequence on the Data Subject • With technical intervention on the part of GSIS • With minor interruption of service to affected Data Subject and other Stakeholders of GSIS • With need to notify Data Subject and report the breach to NPC • Might require further investigation by authorities	• With critical consequence on the Data Subject • With operational and technical intervention on the part of GSIS • With interruption of service to affected Data Subject and other Stakeholders of GSIS • With need to notify Data Subject and report the breach to NPC • Will require further investigation by authorities
IMPACT	4 – LOW	• Personal information or sensitive personal information of less than 100 stakeholders were compromised in a data breach. • Encrypted data; cannot directly relate the compromised information to the Data Subject	P4 – LOW	P4 – LOW	P3 – LOW	P4 – MED

	3 – MED	• Personal information or sensitive personal information of stakeholders of an Agency were compromised in a data breach • A GSIS application system was compromised • Data is readily readable but cannot be directly linked to the Data Subject	P4 – LOW	P4 – LOW	P3 – MED	P4 – HIGH
	2 – HIGH	• Personal information or sensitive personal information of stakeholders of a GSIS Branch Office or of more than one Agency were compromised in a data breach • More than one application system was compromised • Data can readily ascertain identity of the Data Subject	P4 – MED	P4 – MED	P3 – HIGH	P4 – HIGH

	1 – VERY HIGH	• Personal information or sensitive personal information of all stakeholders were compromised in a data breach • All GSIS application system were compromised • Compromised data may significantly affect or reveal the sensitive conditions or preferences of the Data Subject	P4 – HIGH	P4 – HIGH	P3 – HIGH	P4 – HIGH

PASEGURUHAN NG MGA NAGLILINGKOD SA PAMAHALAAN
(GOVERNMENT SERVICE INSURANCE SYSTEM)
Financial Center, Pasay City, Metro Manila 1308

ACKNOWLEDGMENT RECEIPT FORM

==========

Reference No.: :
Issue No. : :
Issue Date:

==========

A. Name of person reporting the incident

Name :
Contact details :

B. Report received by:

Number of data subjects :
Type of data subjects :
Brief description of incident :
Details: :

==========

For inquiries, please call 847-4747
1-800-8-8474747 (Globe)
1-800-10-8474747 (PLDT/Smart) a Php8.00 fee is charged for every call
Privacy@GSIS : 976-49-00 loc 3681
e-mail address : privacy@gsis.gov.ph

==========

GSIS Government Service Insurance System
Financial Center, Pasay City, Metro Manila 1308

GSIS Memorandum Circular No. 030 Series of 2021
PPG373-21

TO : **HEADS OF CONSTITUTIONAL BODIES; BUREAUS AND AGENCIES OF THE NATIONAL GOVERNMENT; LOCAL GOVERNMENT UNITS; GOVERNMENT OWNED OR CONTROLLED CORPORATIONS; STATE UNIVERSITIES AND COLLEGES; AND ALL OTHERS CONCERNED**

SUBJECT : **MANAGEMENT OF DATA BREACH AND SECURITY INCIDENTS RELATIVE TO DATA PRIVACY AND PROTECTION**

Republic Act (RA) No. 10173, otherwise known as the Data Privacy Act (DPA) is a law that seeks to protect all forms of information, be it private, personal, or sensitive. It is meant to cover both natural and juridical persons involved in the processing of personal information.

Further, to give guidance in managing data breach and security incidents, the National Privacy Commission (NPC) issued NPC Circular 16-03, requiring any natural or juridical person in the government or private sector processing personal data, to promptly notify the NPC and the affected Data Subjects relative to the data breaches and security incidents.

In compliance with RA No. 10173 and NPC Circular No 16-03, GSIS has appointed the Data Protection Officer who shall be accountable for ensuring our compliance to laws and regulations related to data privacy. Also, a Data Breach Response Team (DBRT) was created to manage personal data breaches and security incidents and implement the Policies and Procedural Guidelines (PPG) on the Management of Data Breach and Security Incidents relative to Data Privacy and Protection.

If there are other concerns regarding these guidelines, you may contact us using the information below.

GSIS DATA PROTECTION OFFICER
Mr. Jonathan C. Pineda
(02)976-4914 Email: privacy@gsis.gov.ph

Please be guided accordingly.

ORIGINAL SIGNED
ROLANDO L. MACASAET
President and General Manager

Date signed: SEP 06 2021

CERTIFIED TRUE COPY
MA. RUTH ALMIRA G. VASQUEZ
Records Officer
Office of the Corporate Secretary
10 Sep 2021