



I. INTRODUCTION

Data Privacy Act of 2012 or the Republic Act No. 10173 (the “Act”) aims to protect personal data in information and communication systems both in the government and the private sector.

The Act prohibits the processing of certain categories of personal data other than in exceptional circumstances, and set out prerequisites, which must be fulfilled in order for the processing of personal data to be lawful.

SFA Semicon Philippines Corporation (“SSP”) processes personal data on a daily basis. SSP has adopted this manual to ensure that the processing of personal data within SSP is in compliance with applicable data protection legislation.

II. OBJECTIVE

The objective of this manual is to provide SSP’s employees with a basic understanding of situations, which typically are governed by data protection laws, and thereby enable SSP’s employees to comply with those laws.

This manual shall inform the stakeholders the necessary procedures that they need to follow. In addition to that, they may also exercise their rights under this Act.



TITLE:

DATA PRIVACY MANUAL

Doc. No: SFA-M-004

Rev. No.: 1

Effectivity Date:
April 28, 2021

Page No.: 2 of 12

III. DEFINITION OF TERMS

Data Protection Officer	refers to an individual who monitors all the organization's compliance with the Data Privacy Act.
Data subject	refers to an individual whose personal information is processed
Consent of the data	subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.
Personal Data	refers to all types of personal information
. Data Sharing	disclosure or transfer to another entity of personal data under the custody of a company. The term excludes outsourcing, or the disclosure or transfer of personal data by the company to a contractor
Personal Data Breach	refers to 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.
Filing system	refers to 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



TITLE:

DATA PRIVACY MANUAL

Doc. No: SFA-M-004

Rev. No.: 1

Effectivity Date:
April 28, 2021

Page No.: 3 of 12

Personal information	refers to 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.
. Sensitive personal information	refers to personal information: <ol style="list-style-type: none">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; and4) Specifically established by an executive order or an act of Congress to be kept classified.
Direct marketing	refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals

	TITLE:	Doc. No: SFA-M-004
	DATA PRIVACY MANUAL	Rev. No.: 1
		Effectivity Date: April 28, 2021
		Page No.: 4 of 12

IV. SCOPE AND LIMITATIONS

This Manual shall apply to all employees of SSP and employees of independent contractors contracted out by SSP. It likewise covers software developers and electronic service providers of the Board.

V. PROCESSING OF PERSONAL DATA

1. Collection

The Company collects basic employee information by using the Employee Information Sheet (EIS) with the purpose of maintaining records. Information collected includes full name, address, e-mail address, contact number, civil status, government-mandated benefits number, educational attainment and work experiences. Collection of information is done straightforwardly, without any hidden motive by the Human Resources (HR) Personnel by having the employee fill out the EIS. Consent of the Data subject is obtained and evidenced through written means.

2. Use

Employee information collected shall be used by the Company to maintain records, for creating employee personnel cards and for the monitoring for the reports submitted to associated government agencies.

3. Storage

Employee information is encoded in the HR Master List and in the Company's electronic data base. Hard copies such as the EIS are stored in an orderly manner in the HR & GA Storage Room. The Company also implements appropriate security measures against unlawful destruction, alteration, and disclosure of stored information.

4. Access

Considering the confidentiality of stored information, the Company limits the access to the aforementioned storage means. HR Master List is protected by a password, which known only to selected HR Personnel. The Company's electronic data base also requires a user to have an account to be able to access employee information. Moreover, the HR & GA Storage Room is secured in a way that only selected members of the HR & GA Team can have access to it.

5. Disclosure and Sharing

All personnel who have access to employee information shall maintain the confidentiality of the data made known to them even after cessation of employment. Employee information store in the Company's custody, shall kept private unless otherwise required by the law.

	TITLE:	Doc. No: SFA-M-004
	DATA PRIVACY MANUAL	Rev. No.: 1
		Effectivity Date: April 28, 2021
		Page No.: 5 of 12

VI. ROLES & RESPONSIBILITIES FOR SECURITY MEASURES

The Board of Directors of SSP appointed Mr. Mark Adolf D. Paras, as the Data Protection Officer (the “DPO”). The DPO shall include, among others, the following responsibilities:

1. Ensure the Compliance with the Act and regulations along with this policy and other policies of SSP;
2. Annual review of privacy related guidelines, policies, regulations, and procedures of SSP;
3. Submits the necessary reportorial requirements to the National Privacy Commission (“NPC”) and other relevant agency as prescribe by the law;
4. Coordinate with the relevant officer/s of SSP who are responsible for the information security to safeguard the confidentiality, integrity, and availability of personal data and;
5. Improve the security plans of SSP as needed.

VII. BREACH AND SECURITY MANAGEMENT

Most of the security accidents are considered from the improper use of the internal system, and limited precautions in dealing with SSP’s information security system. The following are the procedures used to prevent the information leakage of the stakeholders:


1. Information Leakage Advance Management Policy

Information Leakage means any documents that could damage SSP’s image and/or property thru any leak in the work related device, internal document/s and other personal information. This can be prevented from happening since the internal document cannot be transfer without the consent of the management and IT Team.

2. Information System Destruction & Scrap

> *Handling of Hard Disc & Unusable Network Device (“N/W”)*

- a. Use Degasser to destroy the data and request the IT team to scrap the hard disc.
- b. Unusable N/W device and old device shall be changed into factory initialization value & collect memory after which the IT will scrap.
- c. Return of PC, the important document/s shall be backed up with the help of the IT manager and he will also be responsible for conducting a full data deletion.

	TITLE:	Doc. No: SFA-M-004
	DATA PRIVACY MANUAL	Rev. No.: 1
		Effectivity Date: April 28, 2021
		Page No.: 6 of 12

3. Life Cycle Finished Data Handling:

For important developer's note or N/W system to work, check the date limit and use the shredder for destruction and scrap

Retention Period:

Document/Data Details	3Months	6Months	1Year	3Year
Monthly Inspection Journal				•
Trouble Action Result				•
Information System Management History			•	
Arrangement Plan			•	
Access Management List		•		
Security Accident Action Result				•
Check List	•			
Information System Scrap History			•	
Software Change Installation History			•	

4. User PC Re-Use


It performs a full data deletion to protect the previous user personal information for re usage.

5. Information System Carrying In & Out Handling

Information system carrying in & out shall have a certain Log for a security accident occurrence analysis material. The user should compose a request form and let the information protection manager to check the in and out document.

6. Information System carrying in subject:

1. Storage medium (HDD, SSD, USB Flash Drive, FDD, Writable CD, Memory)
2. Laptop
3. Personal PC
4. N/W Device & accessible cable (LAN Cable, USB Cable, Serial Cables)

	TITLE:	Doc. No: SFA-M-004
	DATA PRIVACY MANUAL	Rev. No.: 1
		Effectivity Date: April 28, 2021
		Page No.: 7 of 12

7. Information System Carrying Out Subject:

1. Destruction/Scrap information system property
2. Laptop
3. Storage medium

8. User Access Limit

To disconnect the unapproved access of the internal N/W, the request should be based on the proper procedure:

1. N/W access for employees shall be preceded based on MAC+IP and includes the name on the list.
2. External Enterprise Management are:
 - a. Seek IT Team Head's approval if LAN & USB port are to be used;
 - b. The LAN & USB port usage permit shall be checked by IT security manager and;
 - c. Only the Related tasks are to process for preparation of security accident based on management & security policy.
3. Network Connection not Active for a period of time: IP Address will be tagged available if IP Address has no connection for a certain period of time.
4. Consider as illegal N/W collection purpose: proceed to limit the base internal information.

9. Internal leak advance limit policy

Most of information security accident is considered from an internal user's mistake and indecent internal usage. Limit shall be based on each item indicated below and if there is any violation, SSP policy shall be implemented as follows

1. Media Control

Advance media control is needed to prevent information leakage through the media and if system paralysis happened, then the malignant code like Auto run invades

- i. Media Control for Employees: FDD, CD-ROM, USB & External Hard (External transferable memory) shall be blocked and;
- ii. Media Control for Outsourcing companies: in case of using memory card for the needed file for work, a software shall be saved in the IT USB, and return it after usage.



TITLE:

DATA PRIVACY MANUAL

Doc. No: SFA-M-004

Rev. No.: 1

Effectivity Date:
April 28, 2021

Page No.: 8 of 12

2. Remote Access Control:

Remote access might deliver information leakage & hacking chance. If an error occurs, it's hard to find the root-cause thus an advance cut shall be managed thru:

- a. Limit all remote access except maintenance control & permitted user;
- b. Limit remote support tool usage;
- c. Get approval from IT manager for remote support and;
- d. Set an expiration time to cut the remote support/access.

3. P2P/Web Hard Control:

This is needed in advance to protect from the bulk information that might leak due to P2P user's carelessness, and virus or Zombie might invade in- company PC by internal N/W slow phenomenon & unapproved file download.

- a. Network disconnection without any exception if malignant virus detected and/or any information leak: P2P site searching;
- b. Team Head's approval is needed to use the Internet access for work related task and;
- c. The approved web hard user shall keep the expiration time and prohibit the access after the given time.

4. Anti-Virus Installation & Maintenance Control

User shall always protect PC with the latest anti-virus and be safe from malignant code and virus:

- a. Anti-Virus shall be controlled and users shall not change it by themselves;
- b. Anti-Virus scan task shall be frequently done;
- c. Anti-Virus server and user connection status shall be always checked;
- d. Conduct a cut policy for user without Anti-Virus and;
- e. In case of deactivation of Anti-Virus in PC, user must be informed the IT Team to run the windows security update.

5. Windows Security Update

User shall check the weak & urgent update, and be safe from weak point hack and error using IT urgent update or urgent patch due to weak point.

- a. The Window Security Update must be set to auto;
- b. N/W access must be disabled if the PC is not updated and;

	TITLE:	Doc. No: SFA-M-004
	DATA PRIVACY MANUAL	Rev. No.: 1
		Effectivity Date: April 28, 2021
		Page No.: 9 of 12

- c. Contact the IT Team in case a window update is not working properly.

6. Screen Saver

Set screen saver for personal information protection and work secrets

- a. Screen saver must be set if the PC is unattended more than 10 minutes;
- b. Input the password to open PC again and;
- c. Perform a screen change with window (icon) + L when user leaves.

7. User Password Management:

Once password is not set, user might be invaded by Trojan horse or malignant virus, and IT shall work to manage this by:

- a. Requiring to use a unique and more than six (6) digit (with special characters) password;
- b. Prohibiting the use of easy to guess passwords such as Love, forever, and contact numbers;
- c. Changing of password frequency is every two (2) months and in case the password was to others, the user should change it immediately and;
- d. Password is the responsibility of the user

8. Email Control:

User shall understand information leakage possible fishing and malignant code to control.

- a. Refrain from reading the email of unknown sender;
- b. Limit the use of words/phrase;
- c. Refrain from using outside email and;
- d. Immediately report to IT team if an email received leads to a website after opening or if an anti-virus was deactivated.

9. Internet Access Control:

Internet use shall only be limited for work efficiency improvement & should not be used to any harmful websites that may cause problem.

- a. User cannot use the internet if it is not work related and;
- b. User should get a permit from the Department Team Head together with IT Team to use internet.



TITLE:

DATA PRIVACY MANUAL

Doc. No: SFA-M-004

Rev. No.: 1

Effectivity Date:
April 28, 2021

Page No.: 10 of 12

10. Explorer temporal file/ recycle bins management

User shall protect and understand not to leak in company secret and personal information.

- a. Make sure to delete all the personal and company information including in the recycle bin;
- b. Scan the illegal software frequently and conduct training to remove all illegal software and;
- c. Back up all file before deleting except the ones who are no use.

11. Detection & Training

- a. Frequent detection and conduct training on how to remove all illegal software. When software was installed, provide software log sheet to record before using it and;
- b. Check the procedure for freeware software installation, and do not install any additional services offered during the installation.

12. Prohibit using N/W through Smart phone

It shall be controlled in advance to protect information leakage through N/W hacking and 3G network.

- a. Prohibiting using of personal mobile phones thru wireless resources;
- b. Conducting security training to regulate the dangerous access by using tethering;
- c. Prohibiting using blue tooth and;
- d. Prohibiting connecting smart phone to the PC.

13. Save important and personal information files with password: Encrypt the important personal data & information by carefully to prevent any security breach.

- a. Carefully save the personal information and company secret file with password;
- b. Report to part head and IT team if personal information file or company secret file are doubt of leakage

14. Precaution for Internet Use: understand the below details when common PC is used

- a. Prohibit installing unknown Active-X;
- b. Check any additional services when installing free unknown software;
- c. Prohibit entering foreign web site;
- d. Prohibit checking email and personal information (health status, citizenship number & contact number);

	TITLE:	Doc. No: SFA-M-004
	DATA PRIVACY MANUAL	Rev. No.: 1
		Effectivity Date: April 28, 2021
		Page No.: 11 of 12

- e. Prohibit using adult website/s or software/s and;
- f. Prohibit installing explorer tool like guide.

15. Report to IT team and try to secure information if below abnormality occurs:

- a. PC suddenly works slowly;
- b. CPU usage constantly higher than normal;
- c. Accidentally deleted data which contain personal information and confidential files,
- d. when using the internet and suddenly redirect you to another website
- e. Anti-Virus is deactivated;
- f. Software is still running after a normal deletion;
- g. Virus detected by Anti-virus but not able to repair;
- h. Other Anti-virus program is installed and activated without knowing and;
- i. Uninstalled icon is activated and not able to end in right-down display (Tray).

16. User Awareness Training:

Social Engineering Hacking is developed recently due to information security system. User awareness training shall be done to protect from social engineering hacking by providing the training twice a year with a special and regular notice.

Set Auto run of explorer temp file & cookie deletion;

- a. When deleting of personal and company information, the user should delete it permanently
- b. Back up all the important files before deleting, delete the original file if there is no problem.

17. Company policy for Information Leakage.

User information leakage policy may be based on HR policies

- ✓ Follow Security Policy (SR1036-01) # 12.

VII. INQUIRIES AND COMPLAINTS

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the organization, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the organization at SFA Semicon Philippines Corporation located at Panday Pira Avenue, Cor. Creekside Road, Clark Freeport Zone, Pampanga, and briefly discuss the inquiry, together with their contact details for reference.

	TITLE:	Doc. No: SFA-M-004
	DATA PRIVACY MANUAL	Rev. No.: 1
		Effectivity Date: April 28, 2021
		Page No.: 12 of 12

Complaints shall be filed in three (3) printed copies or sent to ssphr@sfasemicon.com, the concerned department or unit shall confirm with the complainant its receipt of the complaint

Revision History			
Revision No.	Reason	Date	Responsible
000	Original Issue	2019.07.30	Mark Paras
001	Provide Revision History thru ISO format	2021.04.28	Daisy A. Malig