	Data Privacy Manual		Document Number: 2P-SS-05.43
	Policies & Guidelines	Department: Human Resource	Effective Date: March 28, 2020
			Revision No 0



Data Privacy Manual

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled


	<h1 style="text-align: center;">Data Privacy Manual</h1> <h2 style="text-align: center;">Policies & Guidelines</h2>		Document Number: 2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0


TABLE OF CONTENTS

	<u>PAGE</u>
1.0 Objective.....	3
2.0 Scope.....	3
3.0 Introduction.....	3
4.0 Definition of Terms.....	3
5.0 Responsibility and Authority.....	8
6.0 Data Privacy Principles.....	8
7.0 Functions of a Data Protection Officer (DPO) and/or Compliance Officer for Privacy.....	9
8.0 Rights of the Data Subject.....	10
8.1 Right to be informed.....	10
8.2 Right to Object.....	11
8.3 Right to Access.....	11
8.4 Right to Correction.....	12
8.5 Right to Erasure or Blocking.....	12
8.6 Right to Data Portability.....	12
8.7 Right to Damages.....	12
9.0 Guidelines for the processing of personal data.....	13
9.1 Collection.....	13
9.2 Usage.....	14
9.3 Access.....	14
9.4 Storage Retention, and Destruction.....	14
9.5 Disclosure or Sharing.....	15
9.6 Security Measures.....	17
10.0 Breach and Security Incidents.....	19
10.1 Data Breach Notification.....	19
10.2 Breach Report.....	19
11.0 Inquiries and Complaints.....	20

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1>Data Privacy Manual</h1>		Document Number:
	<h2>Policies & Guidelines</h2>		2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

1.0 Objective

To provide information and guidelines to all employees of F2 Logistics Philippines, Inc. and F2 Global Logistics, Inc. its affiliates, subsidiaries, and related interests when it comes to data protection and its corresponding security measures, and to lead them in the exercise of their rights under the Data Privacy Act of 2012 and its Implementing Rules and Regulations.

2.0 Scope

All employees, directors, clients, business partners, service providers and all other persons who may have provided personal, sensitive and confidential information to F2 Logistics Philippines Inc. and F2 Global Logistics Inc.

3.0 Introduction

F2 Logistics Philippines, Inc. and F2 Global Logistics, Inc. adhere to meet standards and regulations for data protection. The company believes in the right to data privacy and ensures that the personal information collected from its data subjects are processed using the general principles of transparency, legitimate purpose, and proportionality. The company also adopts this Data Privacy Manual in compliance with the Data Privacy Act of 2012, its Implementing Rules and Regulations and all other relevant policies and issuances of the National Privacy Commission.

4.0 Definition of Terms


Access - refers to an individual's right to see and know about his or her own personal data that the Company holds.

Anonymize - to process a collection of personal data or information such that a natural person cannot be identified on the basis of the output collection of data or information.

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1>Data Privacy Manual</h1>		Document Number: 2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

Collection – refers to the process of gathering, acquiring or obtaining personal information from any source, by any means, in circumstances where the individual is identified or is reasonably identifiable. It includes information that:

- is publicly available information about an identifiable individual that the Company comes across;
- information the Company receives directly from the individual; and
- information about an individual the Company receives from somebody else

Commission - refers to the National Privacy Commission

Company – refers to F2 Logistics Philippines, Inc. and F2 Global Logistics, Inc.

Compliance Officer for Privacy (COP) - refers to an individual that performs some of the functions of a DPO for a branch or sub-office.

Consent - refers to any freely given, specific, informed indication of will where the Data Subject agrees to the collection of his/her Personal, Sensitive Personal or Privileged Information. It can be in the form of written and/or electronic.

Data Privacy Act of 2012 or DPA – refers to Republic Act No. 10173 or the Philippine Data Privacy Act of 2012 and its implementing rules and regulations (IRR).

Data Privacy Manual (“Manual”) - establish policies, and implements measures and procedures that guarantee the safety and security of personal data under the Company’s control or custody, thereby upholding an individual’s data privacy rights.

Data Protection Officer (DPO) –refers to the individual designated by F2 Logistics Philippines, Inc. and F2 Global Logistics, Inc. to be accountable for its compliance with the Act, its IRR, and other issuances of the Commission: provided, that, except where allowed otherwise by Law or the Commission, the individual must be an organic employee of F2 Logistics Philippines, Inc. and F2 Global Logistics, Inc.


Data Processing Systems – refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing

Data Sharing – is the disclosure or transfer to a third party of personal data under the custody of a personal information controller (PIC) or personal information

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

 F2 LOGISTICS LET'S MOVE. NOW.	<h1>Data Privacy Manual</h1>		Document Number: 2P-SS-05.43
	<h2>Policies & Guidelines</h2>		
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

processor (PIP). In the case of the latter, such disclosure or transfer must have been upon the instructions of the PIC concerned. The term excludes outsourcing or the disclosure or transfer of personal data by a PIC to a PIP.

Data Sharing Agreement – a contract, joint issuance, or any similar document that contains terms and conditions of a data-sharing agreement between two or more parties provided that only PICs shall be made parties to a data-sharing agreement.

Data Subject – refers to a living individual whose personal information, sensitive personal information, or privileged information is processed by or on behalf of the Company.

Data Subject Information Request – any request received by the company from a Data Subject or other individual or legal entity who wishes to receive a copy of all the Personal Data related to him/her.

Data Subject - refers to any individual who may have provided personal, sensitive or privileged information to F2 Logistics Philippines, Inc. and/or F2 Global Logistics, Inc.

NPC - refers to the National Privacy Commission

Outsourcing - refers to the disclosure or transfer of Personal Data by the company to a Personal Information Processor (PIP) for the latter's processing, in accordance to the instructions of the company

Outsourcing Agreement - refers to any written contract entered into by the company with a Personal Information Processor (PIP), including its service providers

Disclosure – means rendering personal data accessible, by allowing access to personal data either transferring, distributing, or publishing the personal data.


Personal Data – jointly refers to personal information, sensitive personal information and privileged information

Personal Data Breach (or “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. It occurs also when an unauthorized party

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1>Data Privacy Manual</h1>		Document Number: 2P-SS-05.43
	<h2>Policies & Guidelines</h2>		
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

Personal Data Lifecycle - is composed of collection, usage, access and correction, disclosure and distribution/data sharing, storage and transmission, retention, and disposal and destruction.

Personal Data Processing System - refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.

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 to put together with other information would directly and certainly identify an individual.

Personal Information Controller (PIC) - refers to 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.

Personal Information Processor (PIP) - refers to 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.

Primary Purpose - refers to the dominant or fundamental reason for information being collected in a particular transaction. There can only be one primary purpose of collection for a particular transaction.

Privacy Impact Assessment (PIA) - refers to the process undertaken and used to evaluate and manage the impact on the privacy of a particular project, program, process or measure.


Privileged information - refers to any and all forms of Personal Data, which, under the Rules of Court and other pertinent laws constitute privileged communication.

Processing - refers to any operation or set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1>Data Privacy Manual</h1>		Document Number:
	<h2>Policies & Guidelines</h2>		2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

Related Purpose – includes all the purposes that are directly related purposes as well as certain additional ones.

Required by Law - refers to circumstances where a law (other than the Data Privacy Act of 2012) requires the Company to collect, use or disclose or deny access to personal information.

Security Incident - is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of Personal Data.

Security measures - refers to the physical, technical and organizational measures applied in order to protect Personal Data

Sensitive Personal Information refers to Personal Information which:


- involves an individual's race, ethnic origin, marital status, age, color and religious, philosophical or political affiliations;
- involves an individual's health, education, the genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
- involves an individual's personal contact details, and home address;
- issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation and tax returns; and
- specifically established by an executive order or an act of Congress to be kept classified.

Third-party - All external parties – including without limitation contractors, interns, agents, vendors, service providers, and partners -who have access to the Company's information assets and information systems

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1 style="text-align: center;">Data Privacy Manual</h1> <h2 style="text-align: center;">Policies & Guidelines</h2>	Document Number: 2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020
		Revision No 0

5.0 Responsibility and Authority

5.1 The Chief Resources Officer (CRO) shall be responsible to generate resources and address organizational issues related to privacy. In the event the position of DPO or COP is left vacant, the Chief Resources Officer should provide for the appointment, reappointment, or hiring of his or her replacement within a reasonable period of time.

5.2 The Data Protection Officer (DPO) shall act as the leader for the full implementation of the company's Data Privacy Program and Manual.

Qualifications of a Data Protection Officer:

- a. The DPO should possess specialized knowledge and demonstrate reliability necessary for the performance of his or her duties and responsibilities.
- b. The DPO or COP should have a sufficient understanding of the processing operations being carried out by the Company or its PIP/s, including the latter's information systems, data security and/or data protection needs.
- c. The DPO or COP should be a full-time or organic employee of the Company
- d. The DPO may perform other tasks or assume other functions (e.g., legal counsel, compliance officer, etc.) that do not give rise to any conflict of interest.

6.0 Data Privacy Principles

In the processing of personal data, the company, its employees and PIP's abide by the following principles


Transparency - The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data by the Company, including the risks and safeguards involved, the identity of persons and entities involved in processing his or her personal data, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the Processing of personal data should be easy to access and understand, using clear and plain language

Legitimate Purpose- The processing of personal data by the Company shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1 style="text-align: center;">Data Privacy Manual</h1>		Document Number: 2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

Proportionality- The processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed by the Company only if the purpose of the processing could not reasonably be fulfilled by other means.

7.0 Functions of a Data Protection Officer (DPO) and/or Compliance Officer for Privacy

7.1 Monitor the PIC's or PIP's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:

- a. collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
- b. analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
- c. inform, advise, and issue recommendations to the PIC or PIP;
- d. ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
- e. advice the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;

7.2 Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;

7.3 Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);


7.4 Ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;

7.5 Inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC;

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1 style="text-align: center;">Data Privacy Manual</h1>		Document Number: 2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

- 7.6 Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;
- 7.7 Serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;
- 7.8 Cooperate, coordinate and seek the advice of the NPC regarding matters concerning data privacy and security; and
- 7.9 Perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

8.0 Rights of the Data Subject

8.1 Right to be Informed

The data subject has a right to be informed of whether personal data pertaining to him or her. The data subject shall be notified and furnished with the information indicated before the entry of his or her personal data into the processing system of the PIP;

- a. Description of the personal data to be entered into the system;
- b. Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
- c. Basis of processing, when processing is not based on the consent of the data subject;
- d. Scope and method of personal data processing
- e. The identity and contact details of the PIC;
- f. The period for which the information will be stored; and
- g. The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.


8.2 Right to Object

The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1>Data Privacy Manual</h1> <h2>Policies & Guidelines</h2>	Document Number: 2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020 Revision No 0

profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing.

When a data subject objects or withholds consent, the personal information controller shall no longer process the personal data, unless:

- The personal data is needed pursuant to a subpoena;
- The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or
- The information is being collected and processed as a result of a legal obligation.

8.3 Right to Access

The data subject has the right to reasonable access to, upon demand, the following:

- Contents of his or her personal data that were processed;
- Sources from which personal data were obtained;
- Names and addresses of recipients of the personal data;
- The manner by which such data were processed;
- Reasons for the disclosure of the personal data to recipients, if any; and
- Information on automated processes where the data will, or is likely to, be made as to the sole basis for any decision that significantly affects or will affect the data subject;


8.4 Right to Correction

The data subject has the right to dispute the inaccuracy or error in the personal data and have the PIC correct it immediately and accordingly unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the PIC shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients.

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1>Data Privacy Manual</h1>		Document Number: 2P-SS-05.43
	<h2>Policies & Guidelines</h2>		
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

8.5 Right to Erasure or Blocking

The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.

This right may be exercised upon discovery and substantial proof of any of the following:

- The personal data is incomplete, outdated, false, or unlawfully obtained;
- The personal data is being used for a purpose not authorized by the data subject;
- The personal data is no longer necessary for the purposes for which they were collected;
- The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
- The personal data concerns private information that is prejudicial to a data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
- The processing of personal data is unlawful;
- The PIC or PIP violated the rights of the data subject

Upon the request of the data subject, the PIC may notify third parties who have previously received such processed Personal Data of the data subject's decision to exercise such right.

8.6 Right to Data Portability

If the personal data is processed by electronic means and in a structured and commonly used format and upon his/her request, the data subject shall have the right to obtain from the company a copy of such personal data in an electronic or structured format that is commonly used and allows for further use by the data subject


8.7 Right to Damages

The data subject shall be indemnified for any damages sustained due to inaccurate, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as a data subject

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1>Data Privacy Manual</h1>		Document Number: 2P-SS-05.43
	<h2>Policies & Guidelines</h2>		
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

If a Data Subject would want to invoke their rights, he/she can send a message stating the right/s that he/she would like to invoke to dataprotection.officer@f2logistics.com.

9.0 Guidelines for the processing of personal data

9.1 Collection

The company shall only collect and process the personal data of a data subject with the following conditions:

- the employees must only collect sensitive personal information where the information is necessary for the company's functions
- the identity and contact details of F2 Logistics Philippines Inc. and F2 Global Logistics Inc. as the company collecting and storing the information;
- the fact that he or she is able to gain access to the information and seek correction;
- the purpose for which the information is collected;
- the extent of processing, including, where applicable, the automated processing of his or her personal data for profiling;
- the intended recipients or third parties to which the Company usually discloses information of that kind, including any overseas recipients and the countries in which those recipients or third parties or entities and the countries in which those recipients are likely to be located;
- the fact that he or she may make a privacy complaint and how the Company will deal with it;
- any law that requires the particular information to be collected;
- the main consequences, if any, for an individual if all or part of the information is not provided; and
- the period of retention of his or her personal information after processing.

Collection of Personal Data for Research


The employee may collect personal data for research when:

- The personal data is publicly available; or

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1>Data Privacy Manual</h1>		Document Number: 2P-SS-05.43
	<h2>Policies & Guidelines</h2>		
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

- b. Has the consent of the data subject for the purpose of research; or
- c. Protections are in place and no decision directly affecting the data subject shall be made on the basis of the data collected or processed.

9.2 Usage

The use of personal data shall only be for the purpose of carrying out the business operation of the company. The processing of personal data of data subjects shall be for the following general purposes, among others:

- a. to document and manage company records;
- b. to conduct thoroughness before executing a contract, and to enable the terms of the contract thereafter;
- c. to respond to queries, complaints, and requests;
- d. to provide information about company services
- e. to comply with legal and regulatory requirements

9.3 Access

Only the authorized personnel of the company or PIP/s contracted by the company are allowed to access and process personal data of the Data Subject due to its sensitive and confidential nature. A Data Subject who seeks to access to his/her personal data can send a message stating his/her request for access to dataprotection.officer@f2logistics.com.

9.4 Storage, Retention, and Destruction


The storage of personal data will only be stored as long as it is necessary to carry out a business operation of the company:

- a. for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
- b. for the establishment, exercise or defense of legal claims; or
- c. for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by an appropriate government agency.

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1>Data Privacy Manual</h1> <h2>Policies & Guidelines</h2>	Document Number: 2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020
		Revision No 0

Retention period:

For the Record Retention Schedule (RRS) of our different departments, it can be viewed through the company's Intranet website with the link

<http://f2infra.poweredbyclear.com/Intranet/?q=iso-rm-records>

All files that contain personal data must be securely disposed of, destroyed or permanently de-identify, whether such files are:

- Stored on paper, film, optical or magnetic media; and
- Any computer equipment, such as disk servers, desktop and laptop computers and mobile phones at end-of-life (especially storage media);
- Stored offsite, outsourced, or subcontracted.

9.5 Disclosure or Sharing

The Company's DPO will provide the data subject with access to his or her personal data within a reasonable time after such written request or demand is made, as well as to immediately address a request for correction of his or her personal data by writing to the company through dataprotection.officer@f2logistics.com

Disclosure and sharing of personal data shall be used for a legitimate purpose only. A Data Sharing Agreement or an Outsourcing Agreement shall be created in order to formalize an arrangement that the company would like to enter into.

Consent to Data Sharing


The Data Subject shall be provided with the following information prior to Data sharing:

- the identity of the PIC/s and/or PIP/s that will be given access to personal data;
- the purpose/s of the Data sharing;
- the categories of the personal data concerned;
- the intended recipient/s or categories of recipient/s of the personal data;
- the existence of the rights of the data subject; and
- the other information that would sufficiently notify the data subject of the nature and extent of Data Sharing and manner of processing.

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1>Data Privacy Manual</h1>		Document Number:
	<h2>Policies & Guidelines</h2>		2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

Data Sharing Agreement

A Data sharing agreement shall contain the following:

- the purpose of the agreement;
- the identity of the PIC including the company and the other party
- the type of personal data to be shared
- the PIP and the type of processing that would be performed;
- the options available to the data subject in case there is a violation of his/her rights
- the term of Data Sharing Agreement, which may be renewed, provided that such term or any extension that shall not exceed five years
- the overview of the operational details of the agreement
- the general description of the Security measures
- the method in which the agreement may be accessed by the data subject
- the PIC responsible for addressing any request of a complaint filed by the Data Subject
- the other terms that are agreed upon by the company and the PIC/s

Outsourcing Agreement


An outsourcing agreement shall contain the following:

- the purpose of the agreement;
- the duration;
- the subject matter;
- the type of Personal Data and categories of Data Subjects;
- the obligations and rights of the company;
- the location in which the processing would take place;
- the duties of the PIP

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1 style="text-align: center;">Data Privacy Manual</h1> <h2 style="text-align: center;">Policies & Guidelines</h2>	Document Number: 2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020
		Revision No 0

9.6 Security Measures

A. Organizational Measures

- a. the company shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects, processes, and systems involving the processing of personal data.
- b. the designated Data Protection Officer is Atty. Augustus Caesar Bañares, who is concurrently serving as the Legal Counsel of the organization
- c. formation of the Data Privacy Response Team
This response team is composed of the DPO, COP's and all department heads, and shall be responsible for immediate action in the event of a Security Incident or Personal Data Breach. The DPO shall lead the Data Privacy Response Team


The following are the duties of the Data Privacy Response Team:

1. ensure the implementation of this manual;
2. ensure the management of Security Incidents and Personal Data Breaches;
3. ensure the company's compliance with relevant provisions of the Data Privacy Act together with its implementing rules and regulations and all related government issuances on personal data breach management;
4. assess and evaluate the occurrence of a Security Incident or Personal Data Breach;
5. execute measures to mitigate any adverse effect of a Security Incident or Personal Data Breach;
6. periodically conduct a Privacy Impact Assessment and review existing policies and procedures of the company with regard to data privacy;
7. log every Security Incident or Personal Data Breach
8. prepare annual security incident report
9. convene as an investigation committee to recommend actions if there are violations to this manual

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1>Data Privacy Manual</h1> <h2>Policies & Guidelines</h2>	Document Number: 2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020
		Revision No 0

- d. conduct training or seminars to keep personnel, updated in terms of developments in data privacy and security landscape.
- e. all newly hired employees must be asked to sign a Non-Disclosure Agreement
- f. at the first impact of any business activity wherein personal data is received by any party, they must sign a Data Consent Form (e.g. applicants for employment, clients, business partners, suppliers, etc.)
- g. if in case the Data Consent form shall not apply because the disclosure of personal data is not included in the day-to-day operations of the company, the Confidentiality agreement will be used (e.g. external auditors, possible merger and acquisition, credit investigation, etc.)
- h. this manual will be reviewed at least every year from its issue date or earlier if deemed required

B. Physical Measures

- a. personal data collection may be in electronic or physical format.
- b. all personal data stored by the Company shall be placed in storage rooms with limited access only to selected individuals. Paper-based forms must be stored in filing cabinets with locks. Personal data in electronic format must be stored in a secure server.
- c. only authorized personnel should be allowed inside the storage area and data center.
- d. Positioning of office space or workstation is encouraged to be arranged with considerable spaces between them to maintain privacy and protect the processing of personal data.


C. Technical Measures

- a. encryption of electronic messages that contain personal data and is bounded by the Disclaimer and Confidentiality Notice
- b. there is a process on how the administrative IT credentials are generated, store and managed which is seen in the policies of the Information Technology Department specifically 2P-SS-07.06 System Account Creation and 2P-SS-07.07 User Account Deactivation.

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	<h1 style="text-align: center;">Data Privacy Manual</h1>		Document Number: 2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

10.0 Breach and Security Incidents

10.1 Data Breach Notification

- a. the Commission and affected data subject/s shall be notified by the Data Privacy Response Team, which is composed of COP, respective department heads and is led by the Data Protection Officer, upon the report of the PIC or PIP within seventy-two (72) hours upon knowledge
- b. notification of personal data breach shall be required when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the DPO or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.
- c. depending on the nature of the incident, or if there is delay or failure to notify the Commission may investigate the circumstances surrounding the personal data breach. Investigations may include an on-site examination of systems and procedures.
- d. the notification shall at least describe the nature of the breach, the personal data possibly involved, and the measures taken by the entity to address the breach. The notification shall also include measures taken to reduce the harm or negative consequences of the breach, the representatives of the personal information controller, including their contact details from whom the data subject can obtain additional information about the breach and any assistance to be provided to the affected data subjects.
- e. there shall be no delay in the notification if the breach involves at least one hundred (100) data subjects or the disclosure of sensitive personal information that will harm or adversely affect the data subject.
- f. the Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.


10.2 Breach Report

- a. the DPO shall notify the Commission by submitting a report, whether written or electronic, containing the required contents of the notification.
- b. the report shall also include the name of a designated representative of the PIC or PIP together with his/her contact details

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled

	Data Privacy Manual Policies & Guidelines		Document Number: 2P-SS-05.43
	Department: Human Resource	Effective Date: March 28, 2020	Revision No 0

- c. all security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements.
- d. in the case of personal data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the Data Privacy Response team, headed by the DPO.
- e. in other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the Commission.
- f. a general summary of the reports shall be submitted to the Commission annually.

11.0 Inquiries and Complaints

Data subjects may inquire or request for information pertaining to any matter relating to the processing of their personal data as well as the measures that the company is using to ensure the protection of the said data. Data subjects may also report complaints to this manual, unauthorized access or disclosure of personal data under the custody of the company. In both cases, they may send a message to dataprotection.officer@f2logistics.com to which the Data Privacy Response team would reply within twenty-four (24) hours.

Effectivity

The provisions of this manual are effective this 28th day of March, 2020, until revoked or amended by this company, through a memorandum from the President & CEO.

DDC: This Document is already Approved and Posted on Intranet.

Please refer to printed files for signatures of approvers.

Any printed and saved copy of this document is considered uncontrolled