# **DATA** **OUTSOURCING AGREEMENT**

KNOW ALL MEN BY THESE PRESENTS:

This Data Outsourcing Agreement is entered into this \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ by and between:

**SOCIETY OF GYNECOLOGIC ONCOLOGISTS OF THE PHILIPPINES FOUNDATION, INC. (SGOP),** a corporation duly organized and existing under and by virtue of the laws of the Republic of the Philippines, with principal place of business located at \_\_\_\_\_\_\_\_\_\_\_\_, represented by \_\_\_\_\_\_\_ in her capacity as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ hereafter referred to as the FIRST PARTY.

-and-

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.** a corporation organized and existing under the laws of the Republic of the Philippines, with office address at \_\_\_\_\_\_\_\_, represented by <Name of Representative> in his capacity as <Designation>, hereafter referred to as SECOND PARTY.

The Parties are hereinafter referred collectively as the “Parties” and individually as a “Party.”

**RECITALS:**

1. WHEREAS, the Parties entered into an Agreement for \_\_\_\_\_\_\_ dated \_\_\_\_\_\_\_\_\_\_\_. (the “Agreement”);
2. WHEREAS, the Agreement stipulates that I <Specify the Business Arrangement of both parties>
3. WHEREAS, the Agreement inevitably involves the collection and processing of personal data by \_\_\_\_ on behalf of \_\_\_\_\_\_\_\_\_.

**NOW THEREFORE, the parties agree as follows:**

1. **NATURE OF THIS DATA OUTSOURCING AGREEMENT**

This Data Outsourcing Agreement is a supplement to the Agreement and forms an integral part thereof. Where the terms in relation to data privacy of the Agreement and the Data Outsourcing Agreement are in conflict, this Data Outsourcing Agreement shall prevail.

1. **TERM**

Unless otherwise stated in **Annex 1**, this Data Outsourcing Agreement shall be coterminous with the Agreement.

1. **ADHERENCE TO THE DATA PRIVACY ACT OF 2012**

The Parties hereby adhere to the provisions of Republic Act 10173, otherwise known as the Data Privacy Act of 2012, its Implementing Rules and Regulations, and the issuances of the National Privacy Commission (collectively, “DPA”), recognizing the importance of appropriate privacy protections for data subjects.

1. **DEFINITIONS**
	1. *‘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;
	2. *‘Sensitive Personal Information’* refers to personal information:
* About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
* 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 individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
* 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.
	1. *‘Personal Data’* refers to both personal information, sensitive personal information, and privileged information disclosed by the Sharing Party to the Receiving Party pursuant to the Agreement;
	2. *‘Processing’* 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 modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system;
	3. *‘Data Outsourcing’* is the disclosure or transfer of personal data by a personal information controller to a personal information processor who shall process such personal data upon the personal information controller;
	4. *‘Data subject’* refers to an individual whose personal, sensitive personal, or privileged information is processed;
	5. *‘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. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place;
	6. *‘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. A personal data breach may be in the nature of:
* An availability breach resulting from loss, accidental or unlawful destruction of personal data;
* Integrity breach resulting from alteration of personal data; and/or
* A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.
	1. *‘Personal information controller’* 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. The term excludes:
* A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
* 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 extent of its processing;

* 1. *‘Personal Information Processor’* 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;
	2. *‘Technical, Physical, and Organizational Security Measures’* means those measures aimed at protecting Personal Information transmitted, stored, or otherwise processed against improper, unauthorized, accidental or unlawful processing, destruction or loss, disposal, alteration, disclosure, or access, and against all other unauthorized and unlawful forms of processing.
1. **ROLES OF THE PARTIES**

FIRST PARTY is the Personal Information Controller of the personal data disclosed to SECOND PARTY. SECOND PARTY is a Personal Information Processor, i.e., it processes such personal data upon the instruction of FIRST PARTY.

In the event that either party takes on the role of a Personal Information Controller or Personal Information Processor, as defined under the DPA, such party herein undertakes to implement the necessary measures, and execute its role as Personal Information Controller or Personal Information Processor, as the case may be, in relation to any personal data which comes into its possession by virtue of this Agreement, in accordance with the DPA.

1. **PERSONAL DATA TO BE COLLECTED AND PROCESSED**
	1. SECOND PARTY shall process only the Personal Data listed in **Annex 1** in accordance with the terms of the Agreement. Without need of amending this Data Outsourcing Agreement, FIRST PARTY may at any time modify such list by written instructions to SECOND PARTY, which instructions SECOND PARTY undertakes promptly implement in accordance with the Agreement and this Data Outsourcing Agreement.
	2. The terms of this Data Sourcing Agreement shall apply to personal data in all its forms. It may be on paper, stored electronically, held on film, microfiche, or other media. It includes text, pictures, audio, and video. It covers information transmitted by post, by electronic means, and by oral communication, including telephone and voicemail. It applies throughout the lifecycle of the data from creation, collection, storage, utilization, to disposal. The terms of this Data Outsourcing Agreement apply to all officers, employees, and subcontractors of both Parties where they are performing their duties in relation to the Agreement.
2. **PURPOSES OF PROCESSING**

SECOND PARTY shall process the Personal Data only for the purposes listed in **Annex 1**. Without need of amending this Data Outsourcing Agreement, FIRST PARTY may at any time modify such list by written instructions to SECOND PARTY , which instructions SECOND PARTY undertakes promptly implement in accordance with the Agreement and this Data Outsourcing Agreement.

FIRST PARTY may, at any time and upon written instructions to SECOND PARTY, require SECOND PARTY to process the Personal Data pursuant to and consistent with the following purposes:

Comply with statutory and regulatory requirements, including directives, issuances by, or obligations of FIRST PARTY to any competent authority, regulator, supervisory body, enforcement agency, exchange, court, quasi-judicial body, or tribunal;

Enable FIRST PARTY to exercise sound corporate governance over its businesses, ensure that risks arising therefrom are duly identified, measured, managed and mitigated, and enhance risk assessment and prevent fraud;

To enable FIRST PARTY to conduct audits or investigate a complaint or security threat;

Other legitimate business purposes of FIRST PARTY;

Establish, exercise, or defend FIRST PARTY’s legal claims;

Fulfill any other purposes directly related to the above-stated purposes.

1. **GEOGRAPHIC LOCATION OF THE PROCESSING**

The personal data shall be processed by SECOND PARTY at the geographic location specified in Annex 1.

SECOND PARTY shall, at least thirty (30) days prior to effecting any change in the geographic location, notify FIRST PARTY in writing of such intended change and provide reasonable proof that such change shall not adversely affect the privacy and information security measures currently in place or impact the privacy rights of the data subjects.

FIRST PARTY reserves the right to immediately terminate the Agreement and this Data Outsourcing Agreement should SECOND PARTY fail to notify FIRST PARTY within the period stated, or in FIRST PARTY’s discretion and assessment, fail to provide reasonable proof that such change shall not adversely affect the privacy and information security measures currently in place or impact the privacy rights of the data subjects.

1. **OBLIGATIONS OF FIRST PARTY**
	1. Specify the persons and/or entities authorized to receive, access, process, and/or transmit the information obtained and processed by SECOND PARTY. SECOND PARTY can refuse to give information to persons or entities not designated by FIRST PARTY.
	2. Indemnify, defend, and hold harmless SECOND PARTY as well as its officers and employees from and against all liabilities, costs, expenses, damages and losses suffered or incurred by SECOND PARTY arising from the act of processing personal data where such processing is done in breach of this Agreement.
2. **OBLIGATIONS OF SECOND PARTY**

Pursuant to the requirements of the DPA, SECOND PARTY hereby undertakes to:

* 1. Process the personal data only upon the documented instructions of FIRST PARTY, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;
	2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data;
	3. Implement appropriate security measures and comply with the DPA, its Implementing Rules and Regulations, and other issuances of the National Privacy Commission;
	4. Not engage another Personal Information Processor without prior instruction from FIRST PARTY: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;
	5. Assist FIRST PARTY, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;
	6. Assist FIRST PARTY in ensuring compliance with the DPA, its Implementing Rules and Regulations, and other issuances of the National Privacy Commission, taking into account the nature of processing and the information available to SECOND PARTY;
	7. At the choice of FIRST PARTY, delete or return all personal data to FIRST PARTY after the end of the provision of services relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the DPA or another law;
	8. Make available to FIRST PARTY all information necessary to demonstrate compliance with the obligations laid down in the DPA, and allow for and contribute to audits, including inspections, conducted by FIRST PARTY or another auditor mandated by them;
	9. Immediately inform FIRST PARTY if, in its opinion, an instruction infringes the DPA, its Implementing Rules and Regulations, and other issuances of the National Privacy Commission;
	10. Report all available information to FIRST PARTY within twelve (12) hours from knowledge of, or reasonable belief that, a personal data breach or a security incident has occurred, and extend full cooperation to FIRST PARTY to enable FIRST PARTY to comply with its obligations under the DPA and issuances of the National Privacy Commission, including but not limited to reporting to the National Privacy Commission and notification of data subjects.
1. **SECURITY OBLIGATIONS**

Pursuant to its obligation to maintain the appropriate Technical, Physical, and Organizational Security Measures, SECOND PARTY warrants that, at minimum, it shall have the following security measures:

* 1. **Organizational Security Measures**
		1. That it has a designated individual who functions as data protection officer.
		2. That it has implemented appropriate data protection policies that provide for organization, physical and technical security measures, taking into account the nature, scope, context, and purposes of the processing, as well as the risks posed to the rights and freedoms of data subject.
			1. The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.
			2. The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility.
			3. The policies shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices.
		3. That it shall maintain records that sufficiently describe its data processing system and identify the duties and responsibilities of those individuals who will have access to personal data. Records shall include:
			1. Information about the purpose of the processing of personal data, including any intended future processing or data sharing;
			2. A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing;
			3. General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data;
			4. A general description of the organizational, physical, and technical security measures in place;
			5. The name and contact details of each Party, its representative, the subcontractor (if applicable), and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.
		4. That its employees shall operate and hold personal data under strict confidentiality. This obligation shall continue even upon termination of the employee’s employment.
	2. **Physical Security Measures**
		1. That it has implemented policies and procedures to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media;
		2. That the design of its office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public;
		3. That the duties, responsibilities and schedule of individuals involved in the processing of personal data are clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time;
		4. That it has implemented policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of personal data;
		5. That it has implemented policies and procedures that prevent the mechanical destruction of files and equipment. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.
	3. **Technical Security Measures**
		1. That it has implemented safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;
		2. That it has the ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;
		3. That it performs regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach;
		4. That it has the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
		5. That it has a process for regularly testing, assessing, and evaluating the effectiveness of security measures;
		6. That it encrypts personal data during storage and while in transit, authentication process, and it has implemented other technical security measures that control and limit access.
	4. Compliance with FIRST PARTY’s IT Policies and Procedures
		1. SECOND PARTY undertakes to comply with the following IT policies and procedures of FIRST PARTY, which are hereby incorporated by reference into this Data Outsourcing Agreement, as applicable.

Example:

* Physical Security Policy
* Back-up Policy
* Access Management
* Change Management
* Intrusion Detection and Prevention Policy

including any amendments, modifications, or supplement to these policies and procedures, duly notified in writing to SECOND PARTY from time to time. FIRST PARTY may also notify SECOND PARTY in writing of additional IT policies and procedures, in which case, it shall allow SECOND PARTY a reasonable period to comply with the same.

1. **INDEMNIFICATION**

SECOND PARTY agrees to irrevocably, unconditionally, and fully indemnify and hold FIRST PARTY, its officers, employees, and agents, free and harmless from and against any and all claims, suits, actions or demands or losses, damages, costs and expenses including, without limiting the generality of the foregoing, attorney’s fees and costs of suit that FIRST PARTY may face, suffer or incur by reason or in respect of:

* SECOND PARTY’s or its sub-contractor’s breach of any of the warranties and obligations set forth in this Agreement, regardless of the cause of such breach; or
* Any act, omission or negligence of SECOND PARTY or its sub-contractor that causes or results in FIRST PARTY being in breach of its obligations under the DPA.
1. **Data Subject Rights**

Each Party shall respect the following rights accorded to Data Subjects by the Data Privacy Act of 2012:

* 1. Right to be informed. Data subjects have the right to be informed whether personal data pertaining to them shall be, are being, or have been processed, including the existence of automated decision-making and profiling. This Agreement may be accessed by the Data Subject upon written request submitted to any of the Parties.
	2. Right to object. Data subjects have the right to object to the processing of their personal data, including processing for direct marketing, automated processing or profiling. They may withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject.
	3. Right to access. Data subjects have the right to request access to any of their personal data, subject to certain restrictions.
	4. Right to rectification. Data subjects have the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable.
	5. Right to erasure or blocking. Data subjects 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.
	6. Right to damages. Data subjects have the right to be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of the rights and freedoms of the data subject.
	7. Right to lodge a complaint with the National Privacy Commission
1. **Communications Regarding Data Privacy Concerns**

For questions, requests, and notifications, communication may be directed to each Party’s designated Data Protection Officer or his/her replacement or substitute.

* **FIRST PARTY**

**Email:**

**Hotline:**

* **SECOND PARTY**

**Email:**

**Hotline:**

**IN WITNESS WHEREOF,** the PARTIES, through their duly authorized representatives, set their signatures this <DATE> at \_\_\_\_\_\_\_\_\_\_\_\_\_\_ City, Philippines.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| SIGNATURE OVER PRINTED NAME |  | SIGNATURE OVER PRINTED NAME |
|  |  |  |
|  |  |  |

Acknowledgment

REPUBLIC OF THE PHILIPPINES)

\_\_\_\_\_\_\_\_\_\_\_ ) s.s.

BEFOREME, a Notary Public for and in the City of \_\_\_\_\_\_\_ personally appeared the following:

|  |  |  |
| --- | --- | --- |
| Name | Competent Evidence of Identity  | Date & Place of Issue |
|  |  |  |
|  |  |  |

who were identified by me through competent evidence of identity to be the same persons described in the foregoing instrument, who acknowledged before me that their respective signatures on the instrument were voluntarily affixed by them for the purposes stated therein, and who declared to me that they have executed the instrument as their free and voluntary act and deed and of the entities they respectively represent.

This instrument refers to a Data Outsourcing Agreement consisting of eight (8) pages including the page on which this Acknowledgment is written, signed by the authorized representatives of the Parties and their witnesses on the signature page and initialed on each and every other page.

Witness my hand and seal this \_\_\_ day of \_\_\_\_\_\_\_\_ 2021.