

CONTROLLER-PROCESSOR AGREEMENT

Preambles

- (a) Where the Data Controller **Mr George Fenech** requires the Data Processor **(Name of Staff Nurse)** to provide it with data processing services as part of the obligations of the Data Processor pursuant to the Contract (if there is a contract, include name of solution/service/contract).
- (b) Whereas the Data Processor is willing to provide these Services to the Data Controller.

1 Definitions

‘Business Purpose/ Purpose’ means the purpose/s specified in Annex A (Purposes for which the Data Processor may process Personal Data).

‘Confidential Information’ means such data as defined in Clause 6 of this Agreement.

‘Data Protection Legislation’ means the General Data Protection Regulation (EU) 2016/679 (GDPR), and the Data Protection Act 2018 (Cap 586) on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data whether held electronically or in manual form.

‘Data Controller / Controller’ shall have the same meaning of ‘controller’ as set out in the GDPR.

‘Data Loss Event’ means any event that results, or may result, in unauthorised access to Personal Data held by the Data Processor under this Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

‘Data Processor / Processor’ shall have the same meaning of ‘processor’ as set out in the GDPR.

‘Data Processor System’ means the information and communication technology used by the Data Processor in the provision of the Service.

‘Data Protection Impact Assessment’ means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

‘Data Subject’ shall have the same meaning of ‘data subject’ as set out in the GDPR.

‘Data Subject Access Request’ means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

‘Personal Data’ shall have the same meaning of ‘personal data’ as set out in the GDPR.

‘Personal Data Breach’ shall have the same meaning as set out in the GDPR.

‘Process’ shall have the same meaning of ‘processing’ as set out in the GDPR.

‘Protective Measures’ means the measures to be taken by the Data Processor in line with Article 32 of the GDPR to protect against Personal Data Breaches, including technical and organization measures which may include pseudonymizing and encrypting, measures to ensure confidentiality, integrity availability and resilience of systems and services, and measures to ensure that availability of and access to Personal Data can be restored in a timely manner after an incident, and measures to regularly assess and

evaluate the effectiveness of the measures adopted by it.

‘Service’ means the service to be provided by the Data Processor to the Data Controller as detailed in the **main Contract (to include details of the main contract)**.

‘Sub-Processor’ means any third party appointed to process Personal Data on behalf of the Data Controller related to **the Contract/this Agreement**.

‘Software’ shall have the same meaning as **for System Software: Programs like operating systems (Windows, macOS) that run the computer's hardware and provide a base for other programs and. Application Software: User-focused programs designed to perform specific tasks, such as web browsers, word processors. These shall be installed by OPSA in OPSA laptop to be used during the contract for OPSA services.**

2 Scope

- 2.1 The Parties agree that the terms and conditions set forth in this Agreement shall regulate the transfer and processing of Personal Data from the Data Controller to the Data Processor.

3 Data Protection Obligations

Processing

- 3.1 The Data Controller hereby authorises the Data Processor to process Personal Data only to the extent, and in such a manner, as is necessary for the Business Purpose and in accordance with the instructions as detailed in Annex A and subject to the security measures as detailed in the Contract / Annex B The Parties will ensure that any amendments to Annex A and the security measures are to be carried out through a **contract amendment and/or through an amendment to this Agreement that is to be annexed to this document. The Data Processor shall not process Personal Data for any other purpose or without any specific written instructions from the Data Controller.**
- 3.2 The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction of the Data Controller infringes the Data Protection Legislation.

Provided that, in the case only where any act or execution of an instruction falls outside the duties and obligations assumed by the Data Processor in terms of the Contract, the Data Processor shall have the right to refuse carrying out any act and/or the execution of any instruction which, in its opinion, will result in an infringement to Data Protection Legislation and such refusal shall not constitute a breach to this Agreement, subject that such refusal must be accompanied by a written notice spelling out the reasoning behind such a decision as provided at law.

Access to Personal Data

- 3.3 The Data Processor shall ensure that access to the Personal Data is limited to:
- (a) those employees who need access to the Personal Data for the Purpose identified in Annex A; and
 - (b) provided that such employee is granted access only to such part or parts of the Personal Data that is strictly necessary for performance of that employee's duties.
- 3.4 The Data Processor shall ensure that all employees:
- (a) are informed of the confidential nature of the Personal Data;
 - (b) have undertaken training in the laws relating to the handling of Personal Data; and

- (c) are aware both of the Data Processor's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

3.5 The Data Processor shall take reasonable steps to ensure the reliability of any of its employees who have access to Personal Data.

3.6 Where the Data Controller is not satisfied with the performance of the Data Processor's personnel providing the Service, the Data Controller shall immediately notify the Data Processor in writing giving reasons for its dissatisfaction, and the Data Processor shall use its best endeavours to rectify the situation. For the purposes of this clause the performance of the employee shall be deemed unsatisfactory, inter alia, where: (i) such employee is incompetent; (ii) such employee is negligent in the performance of his duties; (iii) lacks the skills and experience required; or (iii) his behaviour at the place of work is unacceptable or unsuitable.

Retention Period

3.7 Retention periods for all categories of personal data processed are to be established by the Data Controller and adhered to by the Processor, keeping in mind Data Protection principles relating to storage limitation. As per the Regulation, such retention periods will not apply to statistical or anonymised data.

3.8 The Data Processor shall ensure that data is securely disposed of upon the lapse of the stipulated retention period.

Data Protection Impact Assessment

3.9 The Data Processor shall, as requested by the Controller, provide all reasonable assistance to the Data Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Data processor and after taking into account the nature of the processing and the information available to the processor, include: (a) a systematic description of the envisaged processing operations and the purpose of the processing; (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services; (c) an assessment of the risks to the rights and freedoms of Data Subjects; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

Data loss Event and Personal Data Breaches

3.10 The Data Processor shall immediately inform the Data Controller of any Data Loss Event, Personal Data Breach(es) and/or if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable in the course of providing the Services in accordance with this Agreement.

3.11 The Data Processor as soon as reasonably practicable, must provide the Controller with the full details (using such reporting mechanism as specified by the Controller from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

3.12 The Data Processor shall fully comply with the provisions of Article 33 of the General Data Protection Regulation, including, but not limited to, keeping a log of such breaches.

Transfer of Data outside the EU

3.13 The Data Processor shall not transfer Personal Data outside the EEA unless the prior written approval of the Data Controller is provided.

Provided that no prior approval shall be necessary for the transfer of data to the United Kingdom in view of the Adequacy Decision adopted by the European Union Commission

on 28 June 2021 in regard to the United Kingdom.

3.14 The Data Processor shall notify the Data Controller immediately if it:

- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
- (b) receives a request to rectify, block or erase any Personal Data;
- (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- (d) receives any communication from the Data Protection Commissioner or any other regulatory / supervisory authority in connection with this Agreement; and
- (e) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purports to be required by law.

The Data Processor's obligation of notification as detailed in this Clause shall include the provision of further information to the Data Controller in phases, as details become available.

3.15 The Data Processor shall provide the Data Controller with full assistance including by promptly providing:

- (i) details and copies of the complaint, communication or request;
- (ii) such assistance as is reasonably requested by the Controller to enable the Controller to comply with Data Subject rights such as requests for access, rectification, and erasure, and other requests such as complaints or communication made by the data subjects, within the relevant timescales set out in the Data Protection Legislation;
- (iii) the Data Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
- (iv) assistance as requested by the Controller following any Data Loss Event;
- (v) assistance as requested by the Controller with respect to any request from the supervisory authorities.

Assistance and Collaboration

3.16 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Controller and Data Processor's obligations laid in the GDPR. The Data Processor shall ensure that it co-operates with any supervisory authority as necessary.

4. Warranty

4.1 Each party warrants to the other that it will process the Personal Data in compliance with the Data Protection Legislation and all applicable laws, enactments, regulations, orders, standards and other similar instruments.

5 Security and Auditing

5.1 The Data Processor shall assist the Data Controller in ensuring compliance with the obligations as detailed in Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the Data Processor.

5.2 The Data Processor warrants that, having regard to the state of technological development and the cost of implementing any measures, it will take Protective Measures against the unauthorised or unlawful processing of Personal Data and against the

accidental loss or destruction of or damage to Personal Data to ensure a level of security appropriate to:

- (a) the risk of and/or the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;
- (b) the nature of the data to be protected including, but not limited to, the security measures set out in the Contract/Annex B.

5.3 The Data Processor shall create and maintain complete and accurate records as detailed in Article 30 of the GDPR.

5.4 The Data Processor shall make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

6 Confidentiality Obligations

6.1 The Data Processor acknowledges that the Personal Data is Confidential Information.

6.2 The Data Processor shall not:

- (a) make copies of the Personal Data, unless approved in writing by the Data Controller;
- (b) extract, re-utilise, use, redistribute, re-disseminate, copy or store the Personal Data other than for the Business Purpose; or
- (c) disclose any Confidential Information in whole or in part to any third party, except as expressly permitted by this clause.
- (d) exploit personal data for any reason whatsoever.

6.3 The Data Processor may disclose Confidential Information to the extent required by law, by any governmental or other regulatory authority, or by a court or other authority of competent jurisdiction provided that, as far as it is legally permitted to do so, it gives the Controller as much notice of the disclosure as possible.

6.4 The Data Controller reserves all rights in its Confidential Information. No rights or obligations in respect of Confidential Information, other than those expressly stated in the main Contract/ this Agreement, are granted to the other party, or are to be implied from the main Contract/this Agreement.

6.5 The provisions of this clause shall continue to apply after termination of the main Contract /this Agreement.

7 Indemnity

7.1 Each party agrees to indemnify and keep indemnified and defend at its own expense the other party against all costs, claims, damages or expenses incurred by the other party or for which the other party may become liable due to any failure by the first party or its employees or agents to comply with any of its obligations under the main Contract/this Agreement.

8 Appointment of Sub-processors

The Data Controller hereby acknowledges that the Data Processor shall **NOT** employ sub-processors to assist it in the data processing activities as detailed under the main Contract/this Agreement and further confirms that it consents to their appointment.

9 Term and Termination

- 9.1. Any provision of this Agreement that expressly or by implication is intended to come into or continue in force on or after termination of the main Contract/this Agreement shall remain in full force and effect.
- 9.2. Termination of the Contract/this Agreement, for any reason, shall not affect the accrued rights, remedies, obligations or liabilities of the parties existing at termination.
- 9.3. On any termination of the main Contract/this Agreement for any reason or expiry of the Term:
- (a) the Data Processor shall as soon as reasonably practicable return (as directed in writing by Data Controller) all Personal Data. The Data Processor shall use reasonable commercial efforts to fulfil such request within ten working days (10) days of its receipt; or
- (b) if the Data Controller elects for destruction rather than return of the materials the Data Processor shall ensure that all Personal Data is immediately deleted from the Data Processor System.
- 9.4. The Data Processor shall provide written confirmation (in the form of a signed letter) no later than fourteen (14) days after termination or expiry of the Contract/this Agreement of compliance with Clause 9.3.

Authorised Signature	Authorised Signature
Name Mr George Fenech	Name
Title CEO	Title
Date	Date
Name of Data Controller	Name of Data Processor

Annex A: Purposes for which the Data Processor may process Personal Data

Description	Details
Business Purpose (generic description of the purpose of the sharing of personal data)	To assist Older Persons Standards Authority (OPSA) in its work as a regulatory body designed to oversee, inspect, and set quality standards for geriatric and residential elder care facilities according to Act No. XXXVIII of 2023 Duties include: to assess, recommend best practices and investigate and resolve health related complaints and issues related to care and health of older persons residing in care homes licensed by OPSA. Details at clause 3 of the EOI agreement. Staff nurse shall be empowered by OPSA to access: • Medical records, including residents' health information and related medical conditions. • Medical complaints received by OPSA.
Duration of the processing (e.g. throughout the Contract/Business Purpose)	Duration of contract to be one (1) year from the engagement date, or until the total amount of 245 hours of conducting assessments and submitting reports are used.
Nature and purposes of the processing (i.e. why is it lawful to process such data: six lawful basis for processing (Consent / Contract / Legal Obligation / Vital Interests / Public Task / Legitimate Interest). If there is processing of special category of data, you need to identify the general purposes for lawful processing as well as the special purpose for such processing. Same applies if we are processing criminal convictions – we need a specific reason. (Please refer to articles 9 and 10 of the GDPR).	To assist OPSA in its duties as per Act No. XXXVIII of 2023 Article 6(1)(c) – Legal obligation and/or Article 6(1)(f) – Legitimate interests. Performance of a task carried out in the public interest (Article 6(1)(e)) as OPSA performs statutory or regulatory functions under Maltese law. Article 9(2)(h) – Occupational medicine, assessment of working capacity, and health management. Article 10 only where complaint investigations involve criminal offence data, and only if the conditions of Article 10 and applicable national law are satisfied
Type of Personal Data Personal Data is broadly defined as data from which a living individual can be identified or identifiable (by anyone), whether directly or indirectly, by all means reasonably likely to be used including names, location data and online identifiers. Special Categories of personal data (special measures have to be taken with Sensitive Data): racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life or sexual orientation, genetic data or biometric data.	Personal data and special category consisting of health-related items
Categories of Data Subject A Data subject is a natural person whose personal data is processed. Categories may include: patients/employees/students/users, etc.	Older persons in residential care homes

Plan for return and destruction of the data once the processing is complete.	Within 10 days from termination of contract.
--	--

Annex B: Security Requirements

Successful applicant

Data Processor should take action for:

- Safeguarding the confidentiality, the integrity, and the availability of the data it is responsible for.
- Reviewing periodically and keeping updated all security requirements indicated in this Annex.
- Continue to receive training on a continuous basis in the provision of the processing of the data in relation to the security requirements listed in this Annex, including training on security awareness.
- Returning upon expiry or termination of the Agreement/Contract any laptop and associated equipment, credentials, keys, tokens and other similar devices required/used for the processing during services to OPSA.
- Ensuring that access rights granted are removed upon expiry or termination of the Agreement/Contract
- Ensuring that physical controls are in place to prevent unauthorised access to the Processor's premises.
- Ensuring that any changes that occur to the processing are carried out through planning, testing and an assessment.
- Ensuring that secure disposal is affected.
- Monitoring of back-ups, capacity and performance on a regular basis.
- Setting-up necessary controls against malicious codes and taking care not to activate phishing links
- Ensuring that the personal data that the controller holds and is accessible by them are stored in a secure manner and physically protected from unauthorised access and damage.
- The staff nurse shall be granted the right to access the personal data, required to execute their duties, that the controller holds, The Processor acknowledges and agrees that the Controller may enable audit logs to monitor and review access rights regularly The Controller may remove access to and disable user accounts at any time.
- Implementing measures to safeguard against the sharing of passwords and implement controls to safeguard the confidentiality of passwords stored in a password management system. Other measures that may be implemented are: the Processor shall not use generic accounts, unless with the prior written approval of the Controller; named accounts shall be assigned to individual personnel; and an account cannot be transferred from one person to another.
- Providing, upon request by the Controller, a report listing all accounts associated with the personnel including their status (active, inactive or deleted) and the reason for such status.

- Ensuring that all personal computers utilised by the personnel are password protected to prevent unauthorised access.
- Ensuring that the papers and storage media containing Controller Data are stored in a secure manner (e.g. in locked cabinets) when not in use, to reduce risks of unauthorised access, loss or damage to the Controller Data.
- Ensuring that in cases where personnel work outside the premises, appropriate security measures are implemented.
- Using test data for testing purposes. Where test data cannot be used, the Processor may, with the prior approval of the Controller, use live data that is sanitised or, only where strictly necessary, use live data on a test environment that shall have the same level of security controls as in the operational environment. However, the Processor must delete any live data once testing is completed and shall inform the Controller in writing of such deletion for audit trail purposes.
- Setting-up and maintaining procedures to monitor, report and manage security incidents and security weaknesses.
- Providing accurate information in a timely manner in the case of an investigation or security breach.