DATA PROCESSING AGREEMENT

This Data Processing Agreement (hereinafter referred to as the “**Agreement**”) is made and entered into on the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_) day of the month of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of the year two thousand and twenty-four (2024) (hereinafter referred to as the “**Effective Date**”).

In virtue of the present private writing between:

**Of the first part**

**[ ]**, a limited liability company organized under the laws of the [ ] bearing company number [ ], having its head office situated at [ ] (hereinafter referred to as the “**Data Controller**”)

**AND**

**Of the second part**

**These Modern Times Limited**, a company incorporated in Malta, bearing company registration number C100505 and registered office at Level 4, The Penthouse, Suite 2, Ewropa Business Centre, Triq Dun Karm, Birkirkara, Malta (hereinafter referred to as the “**Data Processor**”)

(hereinafter collectively referred to as the “**Parties**” or each individually as a “**Party**”)

**WHEREAS**

1. The processing of personal data is regulated by virtue of EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as the “**General Data Protection Regulation**” or the “**GDPR**”) which came into effect on 25 May 2018 as well as the Data Protection Act (Chapter 586 of the Laws of Malta) and any subsidiary legislations thereto (hereinafter cumulatively referred to as “**Data Protection Legislation**” or “**DPL**”);
2. The Data Processor has been engaged by the Data Controller pursuant to the Software License and Services Agreement dated \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (hereinafter referred to as the “**Services Agreement**”) for the provision of a software platform and additional managed services in respect of the optimisation of promotional marketing and customer loyalty through the use of an innovative game concept (the “**Game**” or “**Surprise Me**”) consisting of the possibility of customer to win cashbacks and other prizes, and associated support services (hereinafter referred to as “**Services**”);
3. In order to perform the Services, the Data Processor will require certain Personal Data to be made available to the Data Processor, which Personal Data shall be processed by the Data Processor for and on behalf of the Data Controller strictly for the purposes indicated hereunder;
4. The Parties hereby acknowledge the importance of complying with their respective obligations under the DPL and other applicable data protection laws and wish to enter into a data processing agreement to ensure the proper handling and protection of personal data.

**NOW, THEREFORE,** in consideration of the above recitals, which recitals are expressly made a material part and component of this Agreement, and in further consideration of the promises, covenants, conditions and mutual obligations hereinafter contained, the Parties agree and covenant as follows:

1. **Definitions**
	1. In this Agreement, unless the context otherwise requires, all terms used in this Agreement shall have the same meaning as in the GDPR.
2. **Term**
	1. This Agreement shall commence on the date of execution hereof and shall continue until terminated in accordance with Clause 9 below.
3. **General Requirements**
	1. The Data Processor shall only process the types of Personal Data relating to the categories of Data Subjects for the purposes of the Services Agreement (to the extent necessary to provide the Services) and for the specific purposes in each case as set out in Annex 1 to this Agreement.[[1]](#footnote-1)

Provided that in the event that additional data processing activity/activities is/are identified and/or arise in the future, the respective data processing activity shall be regulated by means of a separate data processing agreement.

Provided further that processing is required by any applicable legislation, laws, rules and/or regulations to which the Data Processor is subject, in which case the Data Processor shall (to the extent permitted by applicable legislation, laws, rules and/or regulations) inform the Data Controller of that legal requirement before the relevant processing of that Personal Data.

* 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall ensure that appropriate technical, physical and organisational measures are taken against unauthorised or unlawful processing of or accidental loss, destruction or damage to Personal Data[[2]](#footnote-2) processed by the Data Processor to ensure a level of security appropriate to the risk exposure, as well as any other minimum security requirements as established in the DPL, including inter alia as appropriate the measures referred to in Article 32(1) of the GDPR, or any other measures as may be communicated to the Data Processor from time to time. The Data Processor shall ensure that such measures are appropriate to the type of data in question and the harm that may result from unauthorised or unlawful processing or accidental loss, destruction or damage to Personal Data and to the nature of Personal Data to be protected.
	2. In assessing the appropriate level of security, the Data Processor shall take into account the risks that are presented by the Processing, particularly from a Personal Data Breach perspective.
	3. Without limitation to the obligations under Clause 3.2 above, the Data Processor shall encrypt all Personal Data being transferred electronically and when stored on any media including all digital or electronic portable storage devices such as computers, laptops, CDs, diskettes, portable drives, magnetic tapes and other similar devices. Personal Data shall be encrypted in compliance with industry best practice and any requirements of applicable DPL.
	4. The Data Processor shall ensure the reliability of employees or other personnel having access to Personal Data and will ensure that access to Personal Data is limited to those of its employees or personnel who require access to it and that such individuals: (i) are subject to user authentication and log‑on processes when accessing Personal Data and (ii) have undertaken training in relation to the DPL and in relating to handling Personal Data; (iii) are informed of the confidential nature of Personal Data and aware of the Data Processor's duties and their personal duties under all applicable laws and this Agreement; and (iv) are subject to confidentiality undertakings, or professional, or statutory obligations of confidentiality[[3]](#footnote-3).
	5. The Data Processor shall not Process or transfer Personal Data to any country outside of the European Economic Area (hereinafter referred to as the “**EEA**”), which has not been recognised by the European Commission as providing an adequate level of protection for Personal Data, without the prior written consent of Data Controller. The Data Processor will procure that the recipient of Personal Data which is located outside of the EEA (including any sub-processor in accordance with Clause 6.4) enters into standard contractual clauses for the transfer of Personal Data from the EU to third countries in the form approved by the European Commission.

1. **The Data Controller’s obligations**
	1. By executing this Agreement, the Data Controller hereby confirms that it has duly assessed and determined that the Data Processor is competent to process Personal data in accordance with the applicable DPL. The Data Controller hereby confirms that it is fully satisfied that the Data Processor can provide sufficient guarantees (in particular, in terms of its expert knowledge, resources and reliability) to implement the appropriate technical and organisational measures to ensure that the processing complies with the applicable DPL and protects the rights and freedoms of Data Subjects.
	2. The Data Controller shall ensure the Processor’s compliance on an ongoing basis, in order for it to satisfy the accountability principle and demonstrate due diligence.
2. **Assistance**
	1. Taking into account the nature of the Processing, the Data Processor shall assist Data Controller, in so far as this is possible, by implementing appropriate technical and organisational measures to facilitate the fulfilment of the Data Controller's obligations (as Data Controller), as reasonably understood the by Data Controller, to respond to requests for exercising Data Subject rights laid down in applicable DPL[[4]](#footnote-4) including promptly complying with reasonable requests from the Data Controller requiring the Data Processor to amend, transfer, dispose or delete Personal Data.
	2. The Data Processor shall notify the Data Controller immediately if it receives a request from a Data Subject under applicable DPL in respect of Personal Data, including for access to that person's Personal Data, and at all times provide full co‑operation and assistance to the Data Controller in relation to any such request in relation to Personal Data being processed by the Data Processor. The Data Processor shall ensure that it does not respond to that request except on the documented instructions of the Data Controller or as required by applicable DPL to which the Data Processor is subject, in which case the Data Processor shall, to the extent permitted by applicable DPL, inform the Data Controller of that legal requirement before the Data Processor responds to the request.
	3. The Data Processor shall immediately notify the Data Controller if any complaint, allegation, assessment, enquiry, notice, investigation or request is made (including by any Regulator) in relation to the Data Processor's processing of Personal Data.
	4. The Data Processor shall provide full cooperation and assistance, as requested by the Data Controller, to enable the Data Controller to reply to any such complaint, allegation, assessment, enquiry, notice, investigation or request[[5]](#footnote-5), which shall include:

### the provision of all data requested by the Data Controller within any reasonable timescale specified by the Data Controller, including full details and copies of the complaint, allegation, assessment, enquiry, notice, investigation or request and any Personal Data it holds in relation to a Data Subject;

### where applicable, provide such assistance as is reasonably requested by the Data Controller to enable the Data Controller to comply with the relevant request within the timeframes prescribed by applicable DPL; and

### implementing any additional technical and organisational measures as may be reasonably required by the Data Controller to allow the Data Controller to respond effectively to relevant complaint, allegation, assessment, enquiry, notice, investigation or request.

## The Data Processor shall make available to the Data Controller on request all information necessary to demonstrate compliance with this Agreement and allow for and contribute to audits mandated by the Data Controller of any premises where the processing of Personal Data takes place and to inspect, audit and copy any relevant records, processes and systems in order that the Data Controller may satisfy itself that the provisions of this Agreement are being complied with[[6]](#footnote-6). The Data Processor shall provide full cooperation to the Data Controller in respect of any such audit and shall at the request of the Data Controller, provide the Data Controller with evidence of compliance with its obligations under this Agreement.

## Provided that the above-mentioned audits and inspections shall be held annually and shall be limited to the processing activities that the Data Processor undertakes on behalf of the Data Processor to ensure minimal disruption to the Data Processor’s operations.

## The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction pursuant to Clause 5.2 infringes the GDPR or any other applicable DPL.

## The Data Processor shall provide reasonable assistance to the Data Controller with any data protection impact assessments (DPIA) if and when such DPIAs are required under Article 35 of the GDPR and with any prior consultations to any supervisory authority of the Data Controller which are required under Article 36 of the GDPR, in each case solely in relation to Processing of Personal Data by the Data Processor on behalf of the Data Controller and taking into account the nature of the Processing and information available to the Data Processor[[7]](#footnote-7).

## With regards to its privacy policy, the Data Controller shall:

### provide the Data Processor with a copy of the latest version;

### in case of additions, amendments and deletions; inform the Data Processor regarding these without undue delay.

## For the instances specified in Clauses 5.8.1 and 5.8.2, the Data Processor shall acknowledge receipt and evidence its acceptance in writing without undue delay.

1. **Disclosures**

## Except under the conditions set forth in Clause 6.2 below, the Data Processor shall not disclose any Personal Data to a third party without the consent of the Data Controller and shall ensure that any such disclosure is made subject to obligations of confidentiality no less protective of Personal Data than those imposed on the Data Processor under this Agreement.

## The Data Processor shall be entitled to disclose Personal Data to the extent required by any mandatory requirement of applicable law provided the Data Processor shall give notice in writing to the Data Controller of any requested disclosure of Personal Data that it is required to make promptly after it becomes aware of such a requirement and in any event prior to making any such disclosure (save to the extent expressly prohibited by any law), such notice to include at least details of the nature and frequency of such disclosures, and shall allow Data Controller to make such representations and/or to participate in the disclosure process to ensure that only Personal Data that is strictly required to be disclosed is disclosed.

## The Data Processor shall not appoint (or disclose any Personal Data to) a sub-processor unless prior written consent of Data Controller is obtained.

## Provided that the Data Controller shall not unreasonably withhold consent in this regard[[8]](#footnote-8).

## With respect to each sub-processor, the Data Processor shall;

* + 1. (before the sub-processor first Processes Personal Data) provide the Data Controller with full details of the Processing to be undertaken by each sub-processor and carry out adequate due diligence on such sub-processor to ensure that it is capable of providing the level of protection for Personal Data as is required by this Agreement, including without limitation sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of applicable DPL, and provide evidence of such due diligence to the Data Controller where requested by the Data Controller or the Regulators;

### ensure that a suitable agreement is in place with such sub-processor and that it includes terms so far as they relate to the processing of Personal Data that are no less protective of Personal Data as the level of protection imposed on the Data Processor under this Agreement. Upon request, the Data Processor shall provide a copy of its agreements with any such sub-processor to the Data Controller for its review (which may be redacted to remove confidential commercially sensitive information not relevant to the requirements of this Agreement);

### remain liable for all the acts and/or omissions of such sub-processor which results in a breach of this Agreement by the Data Processor; and

### insofar as that agreement involves the Processing or transfer of Personal Data outside of EEA, ensure such Processing or transfer is undertaken in accordance with Clause 3.6 above.

1. **Personal Data Breach**
	1. The Data Processor shall notify the Data Controller immediately upon becoming aware of a Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach ("**Original Notification**") and (unless Clause 7.2 applies) provide the Data Controller, at the time of the Original Notification, with sufficient information to allow the Data Controller to meet any obligations to report a Personal Data Breach under applicable DPL. Such notification shall as a minimum:
		1. describe the nature of the Personal Data Breach, the categories and numbers of the Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
		2. communicate the name and contact details of the Data Processor's data protection officer or other relevant contact from whom more information may be obtained;
		3. describe the likely consequences of the Personal Data Breach; and
		4. describe the measures taken or proposed to be taken to address the Personal Data Breach.
	2. If, at the time of the Original Notification, the Data Processor does not have available to it all the information set out in Clauses 7.1.1 to 7.1.4 (both included), the Data Processor shall include in the Original Notification such information as is available to the Data Processor at the time, and then shall provide further information set out in Clauses 7.1.1 to 7.1.4 (both included) as soon as possible thereafter.
	3. Notifications under this Clause 7 shall be sent to the following email address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, subject line “Notification of Personal Data Breach”. The notice shall identify an individual who has sufficient knowledge of the breach and the technical and organisational measures of the Data Processor.
	4. The Data Processor shall co-operate with the Data Controller and take such reasonable commercial steps as are directed by the Data Controller to assist in the investigation, mitigation and remediation of each Personal Data Breach.
	5. In the event of a Personal Data Breach, the Data Processor shall not inform any third party without first obtaining the Data Controller' prior written consent, unless notification is required by applicable law to which the Data Processor is subject, in which case the Data Processor shall, to the extent permitted by such law, inform the Data Controller of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Data Controller before notifying the Personal Data Breach.
	6. The Data Processor shall only be held liable for Personal Data Breaches caused by its own gross negligence or wilful misconduct and shall not be responsible for breaches resulting from actions or instructions of the Data Controller

Provided that the Data Processor reserves the right to reject high-risk processing instructions from the Data Controller if the former deems such instructions to pose a high risk of non-compliance, disproportionality or the materialisation of a Personal Data Breach.

1. **Compliance with Law and Indemnity**
	1. Without limitationto the other provisions of this Agreement the Data Processor shall, at all times, comply with any obligations of the DPL which are applicable to the Data Processor in relation to its processing of Personal Data.

* 1. The Data Processor shall not be held liable for any Personal Data Breaches, unauthorized disclosures, or non-compliance arising from the instructions, decisions, or actions of the Data Controller. The Data Processor's liability shall be limited to instances where it has failed to implement agreed-upon technical and organizational measures or has acted with gross negligence or wilful misconduct. The Data Processor shall promptly notify the Data Controller of any such breaches or non-compliance, and both parties shall cooperate in good faith to mitigate the impact/s and rectify the said breach.
	2. Indemnification for compliance costs: the Data Controller hereby agrees to reimburse the Data Processor for any reasonable costs incurred to ensure compliance with this Agreement and the applicable DPL.
1. **Termination**
	1. This Agreement shall commence on the date executed by the Parties and shall continue, unless terminated earlier in accordance with Clause 9.2, until the successful completion of the provision of the Services to the Data Controller.
	2. The Data Processor shall have the right to terminate this Agreement immediately upon written notice, in the event of termination or expiry of the Services Agreement or due to the Data Controller’s material breach of its obligations under the Services Agreement.
	3. In the event of any termination of this Agreement or the termination or expiry of the Services Agreement, the Data Processor shall:
		1. subject to Clause 9.3.2, immediately cease processing Personal Data; and
		2. promptly return to the Data Controller all of the Personal Data which is in its possession or control and all copies thereof or, at the Data Controller's request, shall destroy all copies of the same and certify to Data Controller that it has done so[[9]](#footnote-9), unless the Data Processor is prevented by law or any regulatory authority from destroying or returning all or part of such data, in which case the Data Processor shall keep such data confidential, continue to process it in accordance with the terms of this Agreement and shall not process it further than required for compliance with such law or regulatory authority.
	4. Termination of this Agreement for whatever reason shall not affect the accrued rights or obligations of any party arising out of this Agreement and all provisions which are expressed to survive this Agreement (or impliedly do so) shall remain in full force and effect.
2. **Assignment and Sub-contracting**
	1. The Data Processor shall not assign, sub‑contract or otherwise transfer its rights or obligations under this Agreement in whole or part to any third party (or purport to do so) without the prior written consent of Data Controller and in accordance with this Agreement.
3. **Entire Agreement**
	1. This Agreement, together with the Services Agreement, constitutes the entire agreement and understanding between the Parties in respect of the matters dealt with in them and supersedes any previous agreement between the Parties relating to such matters.
4. **Precedence**
	1. Nothing in this Agreement reduces the Data Processor's obligations under the Services Agreement in relation to the protection of Personal Data or permits the Data Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Services Agreement. In the event of any conflict or inconsistency between this Agreement and the Services Agreement, this Agreement shall prevail.
5. **Notices**
	1. Any notice required to be given by one Party to this Agreement to the other will be in writing and must be addressed as shown below:

## **The Data Controller:**

## Address: Level 5, 135 Spinola Bay, St. Julians STJ 3093, Malta

## Email: [insert]

## Attention: [insert]

## **The Data Processor**

## Address: [insert]

## Email: [insert]

## Attention: [insert]

## (or unless otherwise notified by the Parties from time to time)

* 1. Notices required under Clause 13.1, will be served by hand delivery or by sending the same by pre-paid first class post or facsimile transmission to (in the case of a letter) the address of such party set out above.
	2. A notice, if:

### delivered by facsimile transmission, shall be deemed to be received on the date of transmission on production of a transmission report by the machine from which the facsimile was sent which indicates that the notice was sent in its entirety to the facsimile number of the recipient;

### sent by prepaid first-class post (airmail, if appropriate), shall be deemed to be given fourteen (14) days after the day on which it was posted; and

### delivered by hand or courier during normal business hours on a business day, shall be deemed to be given on that day, or in any other case of hand delivery or courier, shall be deemed to be given on the business day following the date of delivery.

1. **Waiver**
	1. No waiver of any term, provision, obligation or condition of this Agreement shall be effective except to the extent made in writing and signed by an authorised representative of the waiving party.
	2. No failure or delay by any party to exercise any right or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right or remedy. All such rights and remedies are several and cumulative and not exclusive of each other.
2. **Invalidity**
	1. In the event that any of these terms, conditions or provisions shall be determined by any competent authority to be invalid, unlawful or unenforceable to any extent, such term, condition or provision shall to that extent be severed from the remaining terms, conditions and provisions which shall continue to be valid to the fullest extent permitted by law.
3. **Counterparts**
	1. This Agreement may be executed in any number of counterparts, all of which taken together shall constitute one and the same agreement, and any party may enter into this Agreement by executing a counterpart.
4. **Governing Law and Jurisdiction**
	1. This Agreement and any dispute or claim arising out of or in connection with it (including any non-contractual disputes or claims obligations arising out of or in connection with the same) shall be governed by and construed in accordance with the Laws of Malta. The Parties hereby submit irrevocably to the exclusive jurisdiction of the Maltese Courts in respect of any claim, dispute or difference concerning this Agreement or any matter arising therefrom.

**In** **WITNESS WHEREOF**, this Agreement has been duly executed and delivered as of the day and year first set forth above.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

XXXXXXXXXXXXX XXXXXXXXXXXXX

*for and on behalf of for and on behalf of*

**[ ] These Modern Times Limited**

**ANNEX 1: PERSONAL DATA**

This Annex 1 includes certain details of the Processing of Personal Data as required by Article 28(3) of the GDPR or equivalent provisions of any applicable DPL.

**Subject matter of the Processing of Personal Data**

The subject matter of processing personal data in relation to customers participating the Game encompasses the collection, storage, and analysis of information provided by customers during their engagement with the Game.

**Duration of the Processing of Personal Data**

The processing of personal data of customers participating in the Game shall continue for the duration of their engagement thereto, in line with their explicit consent.

The processing duration is subject to the following conditions:

* Customer Consent: The processing of personal data shall be carried out for as long as customers actively engage in the loyalty game and provide their explicit consent. Customers' consent to the processing of their personal data is obtained during the registration process and reaffirmed with each subsequent interaction within the Game.
* Withdrawal of Consent: Customers retain the right to withdraw their consent for the processing of their personal data at any time. Upon withdrawal of consent, their data shall be promptly anonymized or deleted, unless otherwise required for legal or legitimate business purposes. Further information as to how the customer may exercise his/her right to withdraw his/her consent shall be provided for in our Privacy Policy.
* Termination of the Services Agreement: In the event that a customer's engagement with the loyalty game is terminated due to the expiration of the services agreement or any other reason, the processing of their personal data will cease, and their data will be retained only to the extent required by applicable laws or regulations or for legitimate business purposes.

**The nature and purpose of the Processing of Personal Data**

We collect and process personal data from customers who choose to participate in our customer loyalty game. The purpose of processing this data is to enhance the overall customer experience, tailor marketing strategies, and foster brand loyalty.

**The types of Personal Data to be Processed**

Personal Data that may be processed includes the following:

* Contact details (names, email addresses, phone numbers and mailing addresses during the registration and participation in the Game);
* Preferences and interests (such as preferred products, game achievements, and selected rewards);
* Purchase history (including products acquired, transaction dates, purchase values, which may be used to tailor Game experiences and offers);
* Game interaction data (this involves data generated through customers’ interactions with the Game, including game progress, challenges completed, rewards earned and participation frequency);
* Feedback and communication (information provided by the customers through feedback, reviews, surveys, and other forms of communication related to the Game);
* Demographic information (optional demographic details such as age, gender, and location which may be used for aggregated analysis and customised game content).

**The categories of Data Subject to whom Personal Data relates**

The data subjects shall be those persons who directly engage with the Game and its features, primarily, being the customers who voluntarily participate in the Game.

1. Mandatory requirement - Article 28(3) of the GDPR requires the agreement must set out the subject matter and duration of processing, the nature and purpose of the processing, the type of personal data and categories of data subject and the obligations and rights of the data controller. [↑](#footnote-ref-1)
2. Mandatory requirement - Article 28(3)(c) of the GDPR requires the Data Processor to take all measures required by Article 32 which relates to the security of processing. [↑](#footnote-ref-2)
3. Mandatory requirement - Article 28(3)(b) of the GDPR requires that the data processor must ensure that people processing the personal data are subject to a duty of confidence. [↑](#footnote-ref-3)
4. Mandatory requirement - Article 28(3)e) of the GDPR requires that the data processor must assist the data controller in providing subject access and allowing data subject to exercise their rights under the GDPR. [↑](#footnote-ref-4)
5. Mandatory requirement - Article 28(3)(f) of the GDPR provides that the data processor must assist data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments. [↑](#footnote-ref-5)
6. Mandatory requirement - Article 28(3)(h) of the GDPR provides that the data processor shall submit to audits / inspections, provide the data controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the data controller if it is asked to do something infringing the GDPR or other DPL. [↑](#footnote-ref-6)
7. Mandatory requirement - Article 28(3)(f) of the GDPR provides that the data processor must assist data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments. [↑](#footnote-ref-7)
8. Mandatory requirement - Article 28(3)d) of the GDPR provides that a data processor may only engage a sub-processor with the prior written consent of the data controller and under a written contract. [↑](#footnote-ref-8)
9. Mandatory requirement - Article 28(3)(g) of the GDPR provides that the data processor must delete or return all personal data to the data

controller as requested at the end of the agreement. [↑](#footnote-ref-9)