DATA PROCESSING AGREEMENT

between

[_____]

(the "**Controller**")

and

Hay Systems Ltd ("**HSL**") as Processor

1 INTRODUCTION

The Data Processing Agreement sets out the main principles for processing of Personal Data under, and constitutes an integral part of, the existing agreement for services between the parties (the "**Agreement**").

This agreement document constitutes the data processing agreement between the parties and is in the following referred to as the "**Processing Agreement**".

2 MAIN PRINCIPLES OF PROCESSING OF PERSONAL DATA

2.1 Protection of personal data

HSL takes the matters of protection and security of Personal Data seriously and will process such information in accordance with applicable Data Protection Legislation and the Agreement. In order to provide the services in accordance with the Agreement, HSL may process Personal Data about Users and others who access the services. HSL may disclose Personal Data to third parties as set out in the Agreement.

2.2 Privacy notice

Please refer to the privacy notice for more information about how Personal Data will be processed in relation to the services. The privacy notice is available here: https://hslmobile.com/legal/.

3 PURPOSE OF THE PROCESSING AGREEMENT

The purpose of the Processing Agreement is to regulate rights and obligations pursuant to applicable Data Protection Legislation relating to HSL's processing of Personal Data (as data processor) on behalf of the Controller.

"**Data Protection Legislation**" shall mean the EU General Data Protection Regulation 2016/679 ("**GDPR**") upon entering into force, and national provisions on protection of privacy in the country in which the Controller is established, as amended, replaced or superseded from time to time, including laws implementing or supplementing the GDPR.

"**Personal Data**" means any information relating to an identified or identifiable natural person (the "**Data Subject**").

The Processing Agreement shall ensure that Personal Data is processed in accordance with Data Protection Legislation and is not used unlawfully or comes into the possession of any unauthorized party.

4 SCOPE OF PROCESSING

4.1 General

The Controller determines the purposes and means of the processing of Personal Data.

HSL, its Sub-processors, and other persons acting under the authority of HSL who have access to the Personal Data shall process the Personal Data only on behalf of the Controller and in compliance

with the Agreement and the Controller's documented instructions, and in accordance with the Processing Agreement, unless otherwise stipulated in applicable statutory laws.

HSL shall immediately inform the Controller if, in HSL's opinion, an instruction infringes the Data Protection Legislation.

4.2 The scope of the processing

The Processing Agreement concerns HSL's processing of Personal Data on behalf of the Controller in connection with the provision of the services as further described in the Agreement.

4.3 The purpose of the processing

The nature and the purpose of the processing, including operations and basic processing activities, are to provide the services as further described in the Agreement.

4.4 Categories of Personal Data and Data Subjects

The processing involves processing of Personal Data related to Controller's end-users, customers or employees, depending of the Controller's use of the services.

The Processing relates to the following categories of Personal Data, subject to the Controller's concrete use of the services:

- Basic Personal Data, such as name, contact details such as email, phone number and similar
- Special categories of Personal Data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or health data.
- Location data, such as GPS, Wi-Fi location data and location data derived from HSL's network (that is not traffic data as defined below).
- Traffic data: personal data processed in relation to the conveyance of communication on an electronic communications network or billing thereof.
- Data related to content of communication, such as e-mails, voice mails, SMS/MMS, browsing data and similar

5 OBLIGATIONS OF THE CONTROLLER

The Controller warrants that the Personal Data is processed for legitimate and objective purposes and that HSL is not processing more Personal Data than required for fulfilling such purposes.

The Controller is responsible for ensuring that a valid legal basis for processing exists at the time of transferring the Personal Data to HSL, including that any consent is given explicitly, voluntarily, unambiguously and on an informed basis. Upon HSL's request, the Controller undertakes, in writing, to account for and/or provide documentation of the basis for processing.

In addition, the Controller warrants that the Data Subjects to which the personal data pertains have been provided with sufficient information on the processing of their Personal Data.

Any instructions regarding the processing of Personal Data carried out under this Processing Agreement shall primarily be submitted to HSL. In case the Controller instructs a Sub-processor appointed in accordance with section 12 directly, the Controller shall immediately inform HSL hereof. HSL shall not in any way be liable for any processing carried out by the Sub-processor as a

result of instructions received directly from the Controller, and such instructions result in a breach of this Data Processing Agreement, the Agreement or Data Protection Legislation.

6 CONFIDENTIALITY

HSL, its Sub-processors, and other persons acting under the authority of HSL who have access to the Personal Data are subject to a duty of confidentiality and shall observe professional secrecy in regard to the processing of Personal Data and security documentation pursuant to applicable Data Protection Legislation. HSL is responsible for ensuring that any Sub-processor, or other persons acting under its authority, is subject to such duty of confidentiality.

The Controller is subject to a duty of confidentiality regarding any documentation and information, received by HSL, related to HSL's and its Sub-processors' implemented technical and organisational security measures, or information which HSL otherwise wants to keep confidential. However, Controller may always share such information with supervisory authorities if necessary to act in compliance with Controller's obligations under Data Protection Legislation or other statutory obligations.

The confidentiality obligations also apply after the termination of the Processing Agreement.

7 SECURITY

The security requirements applying to HSL's processing of Personal Data is governed by Appendix 1 to the Processing Agreement.

8 ACCESS TO PERSONAL DATA AND FULFILMENT OF DATA SUBJECTS' RIGHTS

Unless otherwise agreed or pursuant to applicable statutory laws, the Controller is entitled to request access to Personal Data being processed by HSL on behalf of the Controller.

If HSL, or Sub-processor, receives a request from a Data Subject relating to processing of Personal Data, HSL shall send such request to the Controller, for the Controller's further handling thereof, unless otherwise stipulated in statutory law or the Controller’s instructions.

HSL shall assist the Controller for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights stipulated in Data Protection Legislation, including the Data Subject's right to (i) access to its Personal Data, (ii) rectification of its inaccurate Personal Data; (iii) erasure of its Personal Data; (iv) restriction of, or objection to, processing of its Personal Data; and (v) the right to receive its Personal Data in a structured, commonly used and machine-readable format (data portability).

9 OTHER ASSISTANCE TO THE CONTROLLER

If HSL, or a Sub-processor, receives a request for access or information from the relevant supervisory authority relating to the registered Personal Data or processing activities subject to this Processing Agreement, HSL shall notify the Controller, for the Controller's further processing thereof, unless HSL is entitled to handle such request itself.

If the Controller is obliged to perform an impact assessment and/or consult the supervisory authority in connection with the processing of Personal Data under this Processing Agreement, HSL

shall provide assistance to the Controller. The Controller shall bear any costs accrued by HSL related to such assistance.

10 NOTIFICATION OF PERSONAL DATA BREACH

HSL shall notify the Controller without undue delay after becoming aware of a breach related to the processing of Personal Data ("**Personal Data Breach**"). The Controller is responsible for notifying the Personal Data Breach to the relevant supervisory authority.

The notification to the Controller shall as a minimum describe (i) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) the likely consequences of the Personal Data Breach; (iii) the measures taken or proposed to be taken by HSL to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

In the event the Controller is obliged to communicate a Personal Data Breach to the Data Subjects, HSL shall assist the Controller, including the provision, if available, of necessary contact information to the affected Data Subjects. The Controller shall bear any costs related to such communication to the Data Subject. HSL shall nevertheless bear such costs if the Personal Data Breach is caused by circumstances for which HSL is responsible.

11 TRANSFER

Disclosure, transfer or access to Personal Data ("**Transfer**") from countries located outside EU/EEA ("**Third Country**") may only occur in case of approval from the Controller, as described in section 13 below, and is subject to EUs standard contractual clauses between the Controller and the relevant company at the location, or other legal basis for such Transfer.

12 USE OF SUB-PROCESSORS

The Controller agrees that HSL may appoint another processor ("**Sub-processor**"), or a number of processors, to assist in providing the services and processing Personal Data under the Agreement, provided that HSL ensures that:

i) the data protection obligations as set out in this Processing Agreement and in Data Protection Legislation are imposed upon any Sub-processors by a written agreement; and that

ii) any Sub-processor provides sufficient guarantees to implement appropriate technical and organisational measures to comply with Data Protection Legislation and this Processing Agreement, and provide the Controller and relevant supervisory authorities with access and information necessary to verify such compliance.

The Controller hereby specifically approves the appointment of mobile network operators, SMS aggregators, internet service providers and other public electronic communication networks as Sub-processors.

HSL shall remain fully liable to the Controller for the performance of any Sub-processor.

13 PROCEDURE FOR USE OF SUB-PROCESSORS

HSL shall maintain an up-to-date list of the names and contact details of any Sub-processors and locations used by such Sub-processors for processing of Personal Data on the Controller's behalf. HSL shall update the list to reflect any addition or replacement of Sub-processors and, except for specifically approved Sub-processors, notify the Controller at least 3 months prior to the date on which such Sub-processor shall commence processing of Personal Data. Any objection to such changes must be provided to HSL within 3 weeks of receipt of such notification or publication on the website. In case of an objection from Controller as to the supplementing or change of a Sub-processor, HSL may terminate the Agreement and this Processing Agreement with 1 months notice.

By entering into this Processing Agreement, the Controller grants HSL authority to enter into EUs standard contractual clauses on behalf of Controller or to secure other legal basis for Transfer to Third Countries for any Sub-processor approved in accordance with the procedure stipulated above. Upon request, HSL shall provide the Controller with a copy of such EUs standard contractual clauses or description of such other legal basis for Transfer.

HSL shall provide reasonable assistance and documentation to be used in Controller's independent risk assessment in relation to use of Sub-processors or Transfer of Personal Data to a Third Country.

14 AUDITS

HSL shall provide the Controller with documentation of implemented technical and organisational measures to ensure an appropriate level of security, and other information necessary to demonstrate HSL's compliance with its obligations under the Processing Agreement and relevant Data Protection Legislation.

Controller and the supervisory authority under the relevant Data Protection Legislation shall be entitled to conduct audits, including on-premises inspections and evaluations of Personal Data being processed, the systems and equipment used for this purpose, implemented technical and organisational measures, including security policies and similar, and Sub-processors. Controller shall not be given access to information concerning HSL's other customers and information subject to confidentiality obligations.

Controller is entitled to conduct such audits once a year. If Controller appoints an external auditor to perform the audits, such external auditor shall be bound by a duty of confidentiality.

Controller shall bear any costs related to audits initiated by Controller or accrued in relation to audits of Controller, including compensation to HSL for reasonable time spent by it and its employees complying with on premises audits. HSL shall nevertheless bear such costs if an audit reveals non-compliance with the Processing Agreement or Data Protection Legislation.

15 TERM AND TERMINATION

The Processing Agreement is valid for as long as HSL processes Personal Data on behalf of the Controller.

In the event of HSL's breach of the Processing Agreement or non-compliance of the Data Protection Legislation, the Controller may (i) instruct HSL to stop further processing of Personal Data with immediate effect; and/or (ii) terminate the Processing Agreement with immediate effect.

16 EFFECTS OF TERMINATION

HSL shall, upon the termination of the Processing Agreement and at the choice of the Controller, delete or return all the Personal Data to the Controller, including back-up copies, unless otherwise stipulated in applicable statutory law.

HSL shall document in writing to the Controller that deletion has taken place in accordance with the Processing Agreement and as instructed by the Controller.

17 LIMITATION OF LIABILITY

The liability of either party towards the other party under any provision of the Data Processing Agreement or any transaction contemplated by the Data Processing Agreement shall in no event exceed that stated in the agreement entered into between the parties for the provision of services by HSL to the Customer.

18 NOTICES AND AMENDMENTS

All notices relating to the Processing Agreement shall be submitted in writing to the contacts notified under the Agreement.

In case changes in Data Protection Legislation, a judgement or opinion from another authoritative source causes another interpretation of Data Protection Legislation, or changes to the services under the Agreement require changes to this Processing Agreement, the parties shall in good faith cooperate to update the Processing Agreement accordingly.

Any modification or amendment of this Processing Agreement shall be effective only if agreed in writing and signed by both parties.

19 GOVERNING LAW AND LEGAL VENUE

All matters arising under or by virtue of the Processing Agreement shall be governed by and construed in accordance with the law of England and Wales and the parties hereby submit to the exclusive jurisdiction of the courts of England and Wales.

The Processing Agreement is signed in two copies, of which the parties retain one copy each.

For and on behalf of Hay Systems Ltd

_____

To: **Hay Systems Ltd**

We hereby accept and agree to the terms of this Processing Agreement.

…….
Authorised signatory for and on behalf of:

[_____]

Dated ……..

APPENDIX 1 – SECURITY

1 REQUIREMENT OF INFORMATION SECURITY

HSL, which according to the Agreement processes Personal Data on behalf of the Controller, shall implement appropriate technical and organisational measures as stipulated in Data Protection Legislation and/or measures imposed by relevant supervisory authority pursuant to Data Protection Legislation or other applicable statutory law to ensure an appropriate level of security.

HSL shall assess the appropriate level of security and take into account the risks related to the processing in relation to the services under the Agreement, including risk for accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Person Data transmitted, stored or otherwise processed.

All transmissions of Personal Data between HSL and the Controller or between HSL and any third party shall be done at a sufficient security level, or otherwise as agreed between the Parties.

This Appendix contains a general description of technical and organisational measures that shall be implemented by HSL to ensure an appropriate level of security.

To the extent HSL has access to such information, HSL shall provide the Controller with general descriptions of its Sub-processors' technical and organisational measures implemented to ensure an appropriate level of security.

2 TECHNICAL AND ORGANISATIONAL MEASURES

2.1 Physical access control

HSL will take proportionate measures to prevent unauthorised physical access to HSL's premises and facilities holding Personal Data. Measures shall include:

- Procedural and/or physical access control systems
- Door locking or other electronic access control measures
- Alarm system, video/CCTV monitor or other surveillance facilities Logging of facility entries/exits
- ID, key or other access requirements

2.2 Access control to systems

HSL will take proportionate measures to prevent unauthorised access to systems holding Personal Data. Measures shall include:

- Password procedures (including e.g. requirements to length or special characters, forced change of password on frequent basis etc.)
- Access to systems subject to approval from HR management or IT system administrators
- No access to systems for guest users or anonymous accounts
- Central management of system access
- Routines of manual lock when workstations are left unattended, and automatic lock within maximum 5 minutes

- Restrictions on use of removable media, such as memory sticks, CD/DVD disks or portable hard drives, and requirements of encryption

2.3 Access control to data

HSL will take proportionate measures to prevent authorised users from accessing data beyond their authorised access rights, and to prevent the unauthorised access to or removal, modification or disclosure of Personal Data. Measures shall include:

- Differentiated access rights, defined according to duties
- Automated log of user access via IT systems

2.4 Data entry control

HSL will take proportionate measures to check and establish whether and by whom Personal Data has been supplied in the systems, modified or removed. Measures shall include:

- Differentiated access rights based on duties
- Automated log of user access, and frequent review of security logs to uncover and follow-up on any potential incidents
- Ensure that it is possible to verify and establish to which bodies Personal Data have been or may be transmitted or made available using data communication equipment
- Ensure that it is possible to verify and establish which Personal Data have been entered into data-processing systems, altered or deleted, and when and by whom the Personal Data have been input, altered or deleted

2.5 Disclosure control

HSL will take proportionate measures to prevent unauthorised access, alteration or removal of Personal Data during transfer of the Personal Data. Measures shall include:

- Use of state of the art encryption on all electronic transfer of Personal Data
- Encryption using a VPN for remote access, transport and communication of Personal Data
- Audit trail of all data transfers

2.6 Availability control

HSL will take proportionate measures to ensure that Personal Data are protected from accidental destruction or loss. Measures shall include:

- Frequent back-up of Personal Data
- Remote storage
- Use of anti-virus/firewall protection
- Monitoring of systems in order to detect virus etc.
- Ensure stored Personal Data cannot be corrupted by means of malfunctioning of the system
- Ensure that installed systems may, in the case of interruption, be restored
- Uninterruptible power supply (UPS) Business Continuity procedures

2.7 Separation control

HSL will take proportionate measures to ensure that Personal Data collected for different purposes are processed separately. Measures shall include:

- Restrictions on access to Personal Data stored for different purposes based on duties
- Segregation of business IT systems

2.8 Job/subcontractor control

HSL shall implement measures to ensure that, in the case of commissioned processing of Personal Data, the Personal Data is processed strictly in accordance with the Controller's instructions. Measures shall include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

2.9 Training and awareness

HSL shall ensure that all employees are aware of routines on security and confidentiality, through:

- Unambiguous regulations in employment contracts on confidentiality, security and compliance with internal routines
- Internal routines and courses on requirements of processing of Personal Data to create awareness

END