DATA PROCESSING AGREEMENT

This Data Processing Agreement (hereinafter, the "**DPA**") is part of:

- **Factorial**'s terms and conditions; or, as the case may be,
- any other agreement entered into between you and **Factorial** to govern the engagement and use of the Platform (collectively, the "**Agreement**").

This DPA and other provisions of the Agreement are complementary, however, in the event of a conflict, this DPA shall prevail.

I. HOW TO EXECUTE THIS DPA?

This DPA is not signed by **Factorial**. To complete this DPA and receive a signed copy, the Client must:

1. Fill in the appropriate information in the form on page 7.
2. After receipt of a signed copy via email, sign the contract.

Once **Factorial** receives the validly completed and signed DPA from the Client (the "**Effective Date**"), it becomes legally binding.

II. EFFECTIVENESS

This DPA shall apply to personal data processed on your behalf and for your account as Client in the course of your use of the Platform ("**Client Personal Data**").

- The person signing the DPA on behalf of the Client declares to **Factorial** that he/she has the legal authority to bind the Client and that he/she is legally entitled to enter into contracts.
- The term of this DPA shall be the same as the term of the Agreement. This means that this DPA shall automatically terminate upon termination of the Agreement or upon prior termination in accordance with the terms of this DPA.

III. TERMS OF THE DPA

1. Definitions:

The following terms shall have the following meanings:

Factorial", "we", "us", "us", "our" refers to EVERYDAY SOFTWARE, S.L. Spanish company located in calle Àlaba, 61, 5º-2ª, 08005, Barcelona, author, creator and developer of the Platform.

"**Platform"** means our software developed and run on a platform for the purpose of managing an organisation's human resources in the cloud. The Platform is the product provided to you under the Agreement and includes any product we provide to you as part of the Platform.

“Controller", "**Processor**", "**Data Subject**", "**Personal Data**", "**Processing**" and "**appropriate technical and organisational measures"** "**Standard Contractual Clauses**", as used in this DPA, shall have the meanings ascribed to them in the UK GDPR.

"**Client", "you", "your"** refers to the entity contracting the Platform of **Factorial**.

"**End Users"** means the person(s) you permit or invite to use the Platform. For the avoidance of doubt, "End Users" includes the individuals behind accounts managed by you (in particular, your employees).

“**UK GDPR**” means: United Kingdom General Data Protection Regulation.

2. Scope of data protection law.

The parties acknowledge that UK GDPR will only apply to the Client Personal Data that is covered by the definitions contained in such law.

3. Identification of the parties

For the purposes of this DPA:

- **Factorial** shall be considered as the Data Processor.
- The Client shall be considered the Data Controller.

4. Description of the processing and TOMs

A detailed description of the processing to be carried out can be found attached to this DPA as **Appendix 1**. A list of the applicable security standards can be found in **Appendix 2**. A list of the sub-processors that have **FACTORIAL** can be found in **Appendix 3.**

5. **Responsibility of the Client.**

The Client, as the Controller of the Client Personal Data, is responsible for ensuring that its use of the Platform complies with the UK GDPR and for ensuring and monitoring **Factorial**'s compliance with the UK GDPR throughout the processing.

In this regard and prior to contracting the Platform or requesting the activation of additional functionalities, the Client undertakes to determine at its own expense the need to (i) carry out a data protection impact assessment; (ii) carry out the appropriate prior consultations; (iii) as well as any other data protection analyses or assessments. To the extent required under UK GDPR law **Factorial** shall provide the Client with all reasonable assistance in this process or others of a similar nature and purpose.

The Client undertakes to refrain from requesting **Factorial** to contract or activate any functionality of the Platform for which the corresponding data protection impact assessment has given a negative result. The Client exonerates **Factorial** from any liability arising from the Client's failure to comply with this clause.

IV. GENERAL PROVISIONS ON THE PROCESSING OF PERSONAL DATA

In the processing of the Client's Personal Data, **Factorial** commits to comply with the UK GDPR.

The purpose of the data processing shall be exclusively to provide the Platform service on the terms dictated by the Client. This DPA sets out the nature and purpose of the processing, the types of Client Personal Data that Factorial will process and the data subjects whose Client Personal Data will be processed.

In this respect, the processing will be carried out:

- Fulfilling our obligations under Article 28 of the UK GDPR, that is:

  a. process Client Personal Data only in accordance with your documented instructions (as set out in this DPA or the Agreement, or as directed by you through the Platform) for the performance of the service.

  b. by taking the necessary measures in accordance with Article 32 UK GDPR, in the terms set out in Clause VII of this DPA and as set out in Appendix 2.

c. notifying you without undue delay if, in our opinion, an instruction to process Client Personal Data given by you is in breach of UK GDPR law;

d. making available all information reasonably requested in order to demonstrate that our obligations regarding the appointment of sub-processors have been fulfilled, without prejudice to Clause VI;

e. assisting you in fulfilling your obligations under Articles 35 and 36 of the UK GDPR.

f. assisting you in fulfilling your obligations under Articles 15 to 18 of the UK GDPR, providing you with documentation or helping you to retrieve, correct, delete or block Client Personal Data;

g. ensuring that **Factorial** personnel who are required to access Client Personal Data are subject to a binding duty of confidentiality with respect to such Client Personal Data;

h. securely deleting or returning Client Personal Data in our possession following your written request upon termination or early termination of the Agreement, unless retention of the Client Personal Data is required under Union or Member State law;

- In addition, and on the condition that you have previously signed a confidentiality and non-disclosure agreement with **Factorial:**

a. We will allow you and your authorised representatives to access and review documents to ensure compliance with the terms of this DPA.

b. During the term of the Agreement and as required by UK GDPR, we will permit you and your authorised representatives to conduct audits to ensure compliance with the terms of this DPA. Without prejudice to the foregoing, any such audit shall be conducted during our normal business hours with reasonable notice to us and subject to reasonable confidentiality protocols.

The scope of any audit shall not obligate us to disclose to you or your authorised representatives or allow you or your authorised representatives access to: (i) to any data or information of any other **Factorial** client; (ii) any **Factorial** internal accounting or financial information; (iii) any **Factorial** trade secrets; (iv) any information which, in our reasonable opinion, could compromise the security of our systems or facilities; or cause us to breach our obligations under the UK GDPR or our security, confidentiality or privacy

obligations to any other client of Factorial or any third party; or (v) any information which you or your authorised representatives seek to access for any reason other than good faith compliance with your obligations under the UK GDPR and our compliance with the terms of this DPA.

In addition, audits will be limited to once a year, unless we have suffered a security breach in the previous twelve (12) months that has affected Client Personal Data; or an audit reveals a material breach.

V. RIGHTS OF DATA SUBJECTS

If **Factorial,** as processor, receives notice of any claim, complaint, request, direction, enquiry, investigation, proceeding or other action from any data subject, court, regulatory or supervisory authority, or any body, organisation or association, which relates in any way to personal data processed by us on behalf of the Client, Factorial undertakes to:

- notify the Client of this circumstance so that the Client may comply with the request to the extent that such notification is legally permissible;
- provide the Client with reasonable cooperation and assistance; and
- shall not be liable at its own expense, unless the Client is legally obliged to do otherwise in writing.

VI. SUB-PROCESSORS

The Client consents to the use by Factorial of the sub-processors listed in **Appendix 3.** Furthermore, the Client authorises Factorial to engage additional external sub-processors to process the Client's Personal Data.

- The Client must subscribe to receive notifications about the incorporation of new subprocessors by filling this form.

  In the event that the Client objects to the substitution or hiring of a new sub-processor, the parties shall negotiate in good faith alternative solutions that are commercially reasonable.

- **Factorial** requires the new sub-processor to protect the Client's Personal Data to a standard no less strict than that required by this DPA and the UK GDPR.

- Client understands that, by virtue of any confidentiality restrictions that may apply to sub-processors, Factorial may be limited in its ability to disclose sub-processor agreements to Client. In this regard, Factorial undertakes to use all reasonable efforts to require any sub-processor it appoints to allow it to disclose the sub-processor agreement to the Client. Where, despite best efforts, Factorial is unable to disclose a sub-processor agreement to the Client, the parties agree that, upon the Client's request, Factorial will provide, on a confidential basis, such information as it reasonably can in connection with such sub-processor agreement to Client.

VII. SECURITY OF THE PROCESSING

Factorial shall implement and maintain appropriate technical and organisational measures to protect Client Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure, in accordance with the DPA. Such measures shall be appropriate to the harm that could result from any unauthorised or unlawful processing, accidental loss, destruction, damage or theft of the Client Personal Data and appropriate to the nature of the Client Personal Data to be protected. In this sense, **Factorial** may update the technical and organisational measures, provided that such modifications do not diminish the general level of security.

If **Factorial** becomes aware of and confirms any accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access to your Client Personal Data ("**Security Breach**") that we process in the course of providing the Platform we will notify you without undue delay and in any event no later than 48 hours.

VIII. DATA TRANSFERS.

It is part of Factorial's policy to give preference in the contracting of sub-processors to those companies located in the European Economic Area that meet the highest standards of privacy and data protection.

Notwithstanding the foregoing, in the event that Factorial processes Client Personal Data in a country that does not have an adequacy decision (within the meaning of Article 45 UK GDPR), Factorial will adopt an appropriate transfer mechanism in accordance with the UK GDPR.

If Factorial carries out any international transfer for which the transfer mechanism employed is no longer valid under the UK GDPR (e.g. as a result of an invalid court ruling, etc.), the Client shall allow Factorial a reasonable period of time to remedy the breach ("Remediation Period"), in order to identify what additional safeguards or other measures can be taken to ensure its compliance with the UK GDPR.

IX. MISCELLANEOUS.

- The Client acknowledges and agrees that, as part of the provision of the Platform, **Factorial** is entitled to use data relating to or obtained in connection with the operation, support or use of the Platform for its legitimate internal business purposes, such as supporting billing processes, administering the Platform, improving, benchmarking and developing our products and services, complying with applicable laws (including law enforcement requests), ensuring the security of our Platform and preventing fraud or mitigating risk.

  In relation to Client Personal Data, **Factorial** warrants not to use it for its own purposes unless it has aggregated and anonymised the data so that it does not identify the Client or any other person or entity, in particular End Users.

- This DPA is subject to the applicable law and the terms of jurisdiction of the Agreement.

- Without limiting the foregoing, to the extent permitted by applicable law, all liability arising under this DPA shall be governed by the limitations of liability (including caps on liability) in the Agreement.

- In the event that any provision of this DPA is held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not be affected or impaired thereby and such provision shall be ineffective only to the extent of such invalidity, illegality or unenforceability.

- The Client can obtain a copy of this contract signed by Factorial at any time by filling out the following form.

BY FACTORIAL

TITLE	EVERYDAY SOFTWARE, S.L.
SIGNATORY	
AS	
SIGNATURE	

BY THE CLIENT

TITLE	
SIGNATORY	
AS	
SIGNATURE	
DATE	

Appendix 1

(Description of the processing)

Data subjects
Personal data refers to the End Users of the Platform, in addition to individuals whose personal data is provided by the End Users of the Platform.
Data categories
The personal data processed may include the following categories of data: ● Directly identifiable information (e.g. name, e-mail address, telephone number). ● Indirect identification information (e.g. job title, gender, date of birth, user ID). ● Employment information (CV, employment contract, job offer, etc.) ● Financial information (bank account, bank, etc., pay slips). ● Device identification data and traffic data (e.g. IP addresses, MAC addresses, web logs). ● Any personal data provided by users of the Cloud Platform. ● Any personal data contained in a document provided by the Client.
Special categories of data
In the event that the Client requests the activation of the facial recognition functionality for the time clocking of End Users: ● End-User facial image and biometric template
Purpose of processing
Personal data are processed for the purpose of providing the Platform in accordance with the Agreement.
Types of processing
● Collection or recording of personal data. ● Storage or retention of personal data. ● Communication of personal data. ● Use of personal data.

Appendix 2

(Applicable safety standards)

Access control to premises and facilities
● Measures must be taken to prevent unauthorised physical access to premises and facilities containing personal data. Measures shall include: ● Access control system. ● ID reader, magnetic card, chip card. ● (Issuance of) keys. ● Door locking (electric strikes, etc.). ● Surveillance facilities. ● Alarm system, video/CCTV monitor. ● Registration of exits/entries from the premises.
Controlling access to systems
● Measures should be taken to prevent unauthorised access to computer systems. These should include the following technical and organisational measures for user identification and authentication: ● Password protocols (including special characters, minimum length, forced password change). ● There is no access for guest users or anonymous accounts. ● Centralised management of access to the system. ● Access to IT systems is subject to approval by HR management and IT system administrators.
Data access control
● Measures must be taken to prevent authorised users from accessing data beyond their authorised access rights and to prevent the unauthorised input, reading, copying, deletion, modification or disclosure of data. These measures should include: ● Differentiated access rights. ● Access rights defined according to functions. ● Automated logging of user access through computer systems. ● Measures to prevent the use of automated data-processing systems by unauthorised persons using data communication equipment

Disclosure control
● Measures must be taken to prevent unauthorised access, alteration or deletion of data during transfer, and to ensure that all transfers are secure and recorded. These measures shall include: ● Mandatory use of encrypted private networks for all data transfers. ● Encryption via VPN for remote access, transport and data communication. ● Creation of an audit trail of all data transfers.
● **Entry control**
● Measures should be put in place to ensure that all data management and maintenance is recorded, and an audit trail should be kept indicating whether data has been entered, modified or deleted (erased) and by whom. ● Measures should include: ● Logging of user activities in IT systems ● It is possible to verify and establish to which bodies personal data have been or may be transmitted or made available by means of data communication equipment. ● That it is possible to verify and establish what personal data have been entered into automated data processing systems and when and by whom;
● **Control of the order**
● Measures should be put in place to ensure that data are processed strictly in accordance with the controller's instructions. These measures should include: ● Monitoring the execution of the contract
● **Availability control**
● Measures should be put in place to ensure the protection of data against accidental destruction or loss. ● These measures should include: ● Installed systems can, in case of interruption, be restored. ● That systems work and that failures are reported.

- Stored personal data cannot be corrupted by a system malfunction.
- Uninterruptible Power Supply (UPS).
- Business continuity protocols.
- Remote storage.
- Anti-virus/firewall systems.

3. Control of segregation

- Measures should be put in place to allow for separate processing of data collected for different purposes.
- These measures should include:

- Restriction of access to stored data for different purposes according to staff functions.
- Segregation of the company's IT systems.
- Segregation of IT test and production environments.

Appendix 3

(List of sub-processors)

Sub-processors	Function	Country
Amazon Web Services (AWS)	Web Hosting	Frankfurt (Germany)
Amazon Web Services (AWS)	Facial recognition function	Frankfurt (Germany)
Hubspot	Inbound marketing, sales and customer service.	Ireland
Sendgrid (Twilio)	Email Delivery Service	Ireland
Get Site Control	Web traffic conversion	Cyprus
Chargebee	Online Payment Processing	Ireland
Typeform	Tool to improve user interaction through questionnaires.	Spain
Microsoft Clarity	Online data analysis tool that provides information about user behavior on a website.	United States