

End User License Terms (UK - PoV)

1. INTRODUCTION

1.1 Definitions. In these terms the following words have the meanings given below:

client is the entity that accepts these terms when signing up for a “proof of value” trial;

client data is data provided or made available by client or its staff in connection with use of the platform which will include personal data as set out in schedule 1 (*Processing of personal data*);

CultureAI is CultureAI Ltd, English company number 09671771 with registered office at Bold Bauhaus, 2nd Floor, 27 Quay Street, Manchester, England, M3 3GY;

data protection laws are applicable data protection laws, including (without limitation) the Data Protection Act 2018 (**DPA**), the United Kingdom General Data Protection Regulation as defined in section 3(10) and 205(4) of the DPA, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any successor or amending legislation from time to time;

personal data has the meaning given to that term in data protection laws;

platform is the CultureAI cybersecurity platform provided on a software as a service basis from an environment managed by CultureAI and accessed by client from outside that environment;

selected modules are the platform modules to which client is looking to assess as part of the “proof of value” trial;

trial period is a period agreed between CultureAI and Client being at least 7 days commencing on the date nominated by client; and

staff are employees, contractors or other personnel under a person's control.

2. PLATFORM AND CLIENT DATA

2.1 Access and use. CultureAI grants client a non-exclusive, non-transferable and non-sublicensable licence for an agreed number of client's staff to access and use the platform at no cost for the duration of the trial period.

2.2 Warranty. The platform is free of any viruses, trojans or other malware but is otherwise provided ‘as is’ and, to the extent permitted by law, all warranties implied by statute, common law or otherwise are excluded from these terms.

2.3 Permission. Client grants CultureAI permission to collect and process client data to the extent necessary to provide.

2.4 Use. CultureAI shall ensure that no client data made available to the platform is used or accessed other than in accordance with these terms. Personal data collected in connection with the platform will be processed in accordance with schedule 1 (*Processing of personal data*). CultureAI will delete all client data at the end of the trial period.

3. INTELLECTUAL PROPERTY

3.1 Definitions. In this clause the following words and expressions have the meaning given below:

CultureAI materials are materials (i) created by or on behalf of CultureAI prior to or outside the scope of these terms or (ii) comprising machine learning data and/or platform data generated by CultureAI where any personal information has been removed;

intellectual property rights means any intellectual property right or other proprietary right, including copyright, patents, design, database and moral rights, rights in trade and service marks, trade and business names, domain names, confidential information, trade secrets, inventions, software code or know-how, in each case whether registered or not, and in any country;

machine learning data is data including patterns, trends, statistical correlations, and performance metrics derived, generated or inferred through automated processing of platform data and used solely for the purpose of developing, training, testing and improving the platform's machine learning algorithms and associated services; and

platform data is: (i) client data, (ii) other data that describes and/or gives information about client data, including but not limited to metadata, context, files and URLs and (iii) data derived from the platform regarding how it is being used, such as reports and logs.

- 3.2 **CultureAI materials.** All intellectual property rights in the platform, any improvements thereto and all CultureAI materials, vest in and remain with CultureAI and client does not acquire any rights therein save for the permissions expressly granted pursuant to these terms.

4. **CULTUREAI STAFF AND SUBCONTRACTORS**

- 4.1 **Staff.** All CultureAI staff involved in providing the platform or who have access to client data will be bound by confidentiality obligations relating to client data and comply with all applicable laws, regulations and directions of any competent authority in the performance of their role.
- 4.2 **Subcontractors.** CultureAI may use third parties to perform any aspect of these terms but: (i) remains primarily responsible for complying with its obligations hereunder and (ii) shall ensure that contracts with sub-processors comply with the requirements of schedule 1 (*Processing of personal data*) as relevant.

5. **TERM**

- 5.1 **Duration.** The “proof of value” trial expires automatically at the end of the trial period.
- 5.2 **Survival.** All obligations or liabilities accruing prior to expiry of the trial period shall survive such expiration and any clause that is meant to continue thereafter will do so, including but not limited to clause 6 (*Liability*) and 7 (*General*).

6. **LIABILITY**

- 6.1 **Capped liability.** Subject to clause 6.2 (*Unlimited liability*), each party’s total liability arising out of or in connection with the platform or these terms (including but not limited to negligence or breach of statutory duty) is limited to £500.
- 6.2 **Unlimited liability.** Nothing in these terms will limit a party’s liability for: (i) death or personal injury caused by that party’s negligence, (ii) fraud or (iii) anything else that cannot by law be limited.

7. **GENERAL**

- 7.1 **Confidential information.** The parties shall each use the other’s confidential information solely in accordance with these terms and not disclose it except where required by law or regulation.
- 7.2 **Law and jurisdiction.** These terms and any dispute arising from it, whether contractual or not, will be governed by English law and be subject to the exclusive jurisdiction of the English courts.

SCHEDULE 1

PROCESSING OF PERSONAL DATA

1. DEFINITIONS

In this schedule the terms **data subject**, **personal data**, **processing**, **processor** and **supervisory authority** have the meanings given to them in data protection laws and the following words and expressions have the meaning given below:

adequate country is any country determined by the UK Government as providing an adequate level of protection as set out in Section 17A of the DPA; and

incident is any accidental, unlawful, or unauthorised destruction, loss, alteration, processing, disclosure of, or access to any client data (including any personal data) or to any facilities or systems where such data is maintained.

2. PROCESSING

2.1 **Personal data.** In relation to personal data processed in connection with the platform:

- (a) client is the data controller and CultureAI is the data processor for the purposes of data protection laws;
- (b) a description of the personal data processed by CultureAI and its sub-processors is set out at the end of this schedule;
- (c) CultureAI and client will: (i) comply with (and not cause the other to breach) data protection laws, and (ii) promptly (and in any event within 2 business days) inform the other of any relevant notices or requests; and
- (d) CultureAI will: (i) process personal data only as set out in this schedule (and CultureAI shall immediately inform client if, in CultureAI's opinion, an instruction from client infringes data protection laws); (ii) not process or transfer (or allow others to process or transfer) personal data outside the United Kingdom, EEA or another adequate country unless in accordance with applicable data protection laws; (iii) impose a duty of confidentiality on its staff in accordance with clause 4.1 (*Staff*) and implement and maintain appropriate technical and organisational measures for handling client data, including having an information security policy and restricting access to relevant staff only; (iv) provide client with such reasonable information and assistance to enable client to comply with data protection laws in connection with these terms, including in relation to data protection impact assessments, consulting the supervisory authority, data subjects' rights, notifying breaches, submitting to audits and inspections and complying with security obligations and (v) delete or deliver up personal data to client on its request.

2.2 **Incidents.** CultureAI will inform client immediately after becoming aware of an incident, take immediate steps to contain the incident and provide any additional information and assistance as reasonably requested by client.

3. SUBPROCESSORS

3.1 **Authorisation.** CultureAI may engage sub-processors as listed in Annex 1.B below (the **approved sub-processors**) which may be updated from time to time and client provides a general authorisation for CultureAI to engage sub-processors that is conditioned on the following:

- (a) CultureAI will restrict the sub-processor's access to client data only to what is strictly necessary to provide the platform or operate its business, and CultureAI will prohibit the sub-processor from processing client data for any other purpose; and
- (b) CultureAI agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor protect client data to the standard required by data protection laws.

4. DESCRIPTION OF PERSONAL DATA PROCESSED

Annex 1.A (Parties)	
Exporter (Controller):	client
Importer (Processor):	CultureAI
Annex 1.B (Description of Data Processing)	

Categories of data subjects:	client's staff
Categories of personal data transferred:	<p>Personal data collected by the platform through its use by client's permitted users. The baseline data required to provide the platform comprises a permitted user's:</p> <ul style="list-style-type: none"> (a) personal identification (first, last and full name); (b) contact information (company email, job title, business unit or department, working location and line manager); and (c) account information (unique account number, authentication method (e.g. SSO - single sign-on) and password complexity (but not the actual password)). <p>Where certain platform modules have been selected by client the following data is also collected:</p> <p><i>Identity & SaaS Risks</i></p> <ul style="list-style-type: none"> (a) web browser log-in events using company email and web browsing generally in order to identify whether malicious websites are being accessed (data is stored only where a match is made, not all browsing); <p><i>Generative AI Usage</i></p> <ul style="list-style-type: none"> (b) data for personal data detection being certain data attributable to a user's company email login provided to monitored LLMs via the web browser (e.g. Chat GPT, Copilot, Gemini etc.); and <p><i>Collaborative Tool Usage</i></p> <ul style="list-style-type: none"> (c) data for personal data detection being certain data attributable to a user's company email login from instant messages (e.g. from MS Teams, Slack etc.). <p>Further personal data may be processed by the platform where client has requested. No sensitive personal data is intentionally collected by the platform but CultureAI cannot guarantee this might not occur inadvertently where such data has been disclosed by users.</p>
Nature and purpose of the processing:	<p>As necessary for CultureAI to provide the platform which may (where client has selected the relevant module) include operations to facilitate (if selected) detection of personal data and other data specified by client as being particularly sensitive, which may include data from instant messages (e.g. from MS Teams, Slack etc.) or data entered into LLM chats via the browser (e.g. ChatGPT, or Claude.ai).</p> <p>Such operations use functionality provided by AWS (see below).</p>
Duration:	While the platform is being used by client's permitted users.
Sub-processors:	<p>The platform is hosted on Amazon Web Services cloud servers in the EU.</p> <p>DataBricks (also hosted on AWS EU and synchronised to our production environment) provides dashboarding and analytics to administer, maintain and improve the platform. We use ChatGPT Enterprise (which stores information in the EEA or Switzerland only) to perform analytics and to administer, maintain and improve the platform, diagnosing issues and day to day business operations.</p> <p>A limited number of other providers are used to track, diagnose and resolve certain issues clients experience with our platform. The only personal data provided to such sub-processors is the corporate email and sometimes the IP address of the user experiencing the issue. Those platforms are HotJar (AWS EU), DataDog (Germany) and Sentry (US) and these (i) enable us to record end-user sessions to understand user interactions with the platform and (ii) provide crash / error logs to facilitate diagnosis.</p>
Transfer frequency:	Continuous.
Annex 1.C (Competent Supervisory Authority)	
Competent Supervisory Authority:	The UK Information Commissioner but where the exporter is established in an EU Member State, The Irish Data Protection Commissioner.
Annex 2 (Technical and Organisation Measures)	
Technical and organisational measures:	CultureAI shall process personal data in accordance with its information security policy (available on request).