

Supplier Licence Terms

These Oleeo Licence Terms, ("**Supplier Licence Terms**"), apply to all **Products** sold by the Supplier to a Buyer for use by the Buyer pursuant to the Agreement between the Supplier and the Buyer.

IT IS AGREED AS FOLLOWS:

1. Definitions

"Agreement" means the G-Cloud agreement entered into between Supplier and the Buyer, which incorporates each signed Order Form, these Supplier Licence Terms, the Supplier DPA and the Supplier SLA, and any other document referred to in these Supplier Licence Terms;

"Agency User" means a recruitment agent of the Buyer (or Buyer's affiliates) granted limited access to the System's functionality for the purpose of providing recruitment services to the Buyer (or Buyer's affiliates);

"AI Functionality" means the suite of artificial intelligence-powered features and capabilities integrated into the AI Products included in an Order Form that use data analysis, pattern recognition, natural language processing, prediction and automated decision support to process Input to generate Output using AI models of both the Supplier and AI Providers as defined more specifically in Section 10 of these Supplier Licence Terms for each AI Product;

"AI Products" means any Products set out in an Order Form, used by the Buyer or Users that include any AI Functionality;

"AI Providers" means the third party providers of AI Functionality listed in Appendix 1 of these Supplier Licence Terms;

"AI Terms" means the AI terms set out in Section 10 of these Supplier Licence Terms that apply in addition to any AI Functionality.

"System" means the application tracking services platform of the Supplier made available by the Supplier to the Buyer;

"Business Day" means a day other than Saturday, Sunday or public holiday in the UK;

"Business Hours" means hours between 8:00AM and 6:00PM (UK local time);

"Buyer" means the Buyer who entered into the Agreement;

"Buyer Data" means the Database and all data relating to Buyer Users or Candidates of Buyer or their affiliates contained within the System, including all data supplied, processed, stored, derived, input, or output by or on behalf of the Buyer, Buyer Users or Candidates of the Buyer or their affiliates and all data generated by the Buyer, Buyer Users or Candidates of the Buyer or their affiliates through use of the Services or the System;

"Buyer Users" means Registered Users and Agency Users (where applicable);

“Candidate” means any candidate who may be applying for jobs with the Buyer;

“Change Request” means any change to the System and/or Services which is requested by the Buyer;

“Confidential Information” means all information of a confidential nature which relates to any party (including information relating to Buyer affiliates) and including without limitation all information which relates to the business, financial affairs, products, developments, trade secrets, know-how, personnel, customers and suppliers of any party (or Buyer affiliates) or information which may reasonably be regarded as the confidential information of the party disclosing it, that is directly or indirectly disclosed by or on behalf of a party to the other party; For the avoidance of doubt, Buyer Data (including without limitation all personal data processed by the Supplier on behalf of the Buyer or its affiliates) shall be considered Buyer Confidential Information;

“Content” means Input and Output together.

“Database” means the database of Candidate data compiled from their use of the System which the Buyer is able to download from the System;

“Effective Date” means the effective date of each Order Form;

“Input” means all data provided by the Buyer and/or Users or the Supplier, as defined more specifically for each AI Product as set out below, and used by the AI Functionality to produce Output:

(i) for OleeoQ

means all data (which may include personal data) provided by the Buyer, Candidates and/or Users.

(ii) for OleeoQ Candidate Support (only relevant where Oleeo Recruit is purchased)

means all data provided by the Supplier (technical FAQ's)

(iii) for Candidate Navigator

means all data (including personal data) provided by the Buyer and Candidates.

(iv) for Oleeo VacancyIQ

means all data provided by the Buyer and Users. No personal data is included.

(v) for Oleeo SkillsAssess

means all data (including personal data) provided by the Buyer, Candidates and Users.

(vi) for Oleeo Interview Notes

means all data (including personal data) provided by the Buyer, Candidates and Users.

(vii) for Oleeo AI Candidate Screening

means all data (including personal data) provided by the Buyer, Candidates and Users.

(viii) for Oleeo Search & Match

means all data (including personal data) provided by the Buyer, Candidates and Users.

(ix) AI Assistant (only relevant where Oleeo Recruit is purchased)

means (i) all data provided by the Supplier (training material and technical FAQ's) or
(ii) all data provided by the Buyer.

"Intellectual Property Rights" means all intellectual property or similar proprietary rights in any part of the world and shall include but not be limited to: patents (including supplementary protection certificates), utility models, rights in inventions, registered and unregistered trade and service marks, rights in business and trade names and get-up, rights in domain names, registered designs, unregistered rights in designs, semiconductor and topography rights, copyrights and neighbouring rights, database rights, rights in know-how and in each case rights of a similar or corresponding character and all applications and rights to apply for the protection of any of the foregoing;

"Implementation Services" means the development and configuration services to be provided by the Supplier as described in an Order Form;

"Line Manager User" means a Registered User who is not a Recruiter User;

"Order Form" means each order form signed by the Supplier and the Buyer which together, shall be referred to as **Order Forms**;

"Output" means all content or results generated by each AI Product, based on the Input;

"Products" means all products (including AI Products where applicable) set out in an Order Form;

"Professional Services" means any consultancy or other services provided by the Supplier to the Buyer, set out in an Order Form;

"Recruiter User" means a Registered User who is part of the Buyer (or of the Buyer affiliates') internal recruitment department;

"Registered User" means an employee or sub-contractor of the Buyer (or of the Buyer affiliates) granted access to the System's functionality;

"SLA" means the service level agreement of the Supplier applicable between the Supplier and the Buyer, as amended from time to time;

"Subscription" means the license granted to the Buyer to access and use the Products;

"Subscription Term" means the subscription term for the Products, set out each Order Form;

"Supplier" means Oleeo Ltd;

"User" means any user or end user of the Buyer, including Candidates where applicable, who has access to, or uses, the AI Products.

2. Provision of Products

- A.** All Products included in each Order Form shall be provided subject to the provisions of these Supplier Licence Terms.
- B.** The AI Terms shall apply in addition for all AI Functionality.
- C.** The hosting, maintenance and level support services for the System shall be provided to the Buyer in accordance with the terms of the SLA.
- D.** The Buyer is granted a non-exclusive, non-transferable, revocable license to resell non-exclusive, non-transferable, revocable licenses to allow Buyer affiliates and Buyer Users to access the Products via the Internet solely to manage their recruitment requirements.
- E.** The Buyer shall not store, distribute or transmit any material when using the Products that is unlawful, harmful, threatening, defamatory, obscene, harassing or racially or ethnically offensive; facilitates illegal activity; depicts sexually explicit images; or promotes unlawful violence, discrimination based on race, gender, colour, religious belief, sexual orientation, disability, or otherwise illegal.
- F.** The rights provided under this Section 2 are granted to the Buyer and Buyer affiliates only, and shall not be considered granted to other entities unless otherwise specified.
- G.** The Buyer shall not attempt to: (i) duplicate, modify or distribute any portion of the Products; or (ii) attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form any of the Products, except as may be allowed by any applicable law which is incapable of exclusion between the parties; or (iii) use the Products to provide services to third parties (other than Buyer affiliates and Candidates of Buyer and Buyer affiliates'); or (iv) transfer, temporarily or permanently, any of its rights under these Supplier Licence Terms; or (v) attempt to obtain, or assist others in obtaining, access to the Products.
- H.** The Buyer is not permitted to target or permit use of the Products to Users or Candidates who are under 16 years of age.

3. Supplier obligations

- A.** If the System does not conform to the terms of the Agreement, Supplier will, at its expense:
 - (i) use commercially reasonable efforts to correct any such non-conformance;
 - (ii) provide Buyer with an alternative means of accomplishing the desired performance while maintaining the features and functionality of the System; or
 - (iii) if (i) and (ii) are not commercially feasible refund the fees paid by the Buyer on a pro-rated basis taking into consideration the length of time the System was used prior to termination. The foregoing remedies are Buyer's sole and exclusive remedy for any breach of warranty under the Agreement.

- B. The Supplier does not warrant that Buyer, Buyer Users' or Candidates of the Buyer or Buyer affiliates' use of the Products will comply with laws applicable to them any of their business operations.
- C. No warranty is given for : (i) any non-conformance of the Products that is caused by use contrary to the Supplier's instructions; or (ii) modification or alteration of the Products by any party other than the Supplier or its agents.
- D. The Supplier does not warrant that Buyer's use of the Products will be uninterrupted or error-free and the Buyer acknowledges that any tests, questionnaires, or decision rules that are configured within the Products are intended to provide a guide only to the Buyer of the suitability and aptitude of Candidates and accordingly, the Buyer shall be solely responsible for all decisions taken or not taken in respect of Candidates.

4. Buyer Obligations

A. The Buyer shall:

- 1. provide the Supplier with: (i) co-operation in relation to the Agreement; and (ii) access to information necessary for the Supplier to provide the Products, including, but not limited to, Buyer Data, security access information and software interfaces to the Buyer's website.
- 2. comply with all applicable laws and regulations with respect to its activities when using the Products; and
- 3. carry out all their responsibilities in a timely and efficient manner.

- B. If the Buyer fails to comply with its obligations under Section 4.A and the Supplier is required to repeat the provision of any services or perform additional services as a result of such failure, the Supplier shall be entitled to charge the Buyer fees at its standard rate for Professional Services on a time and materials basis; provided, however, that: (i) the Supplier shall be required to provide advance written notice of such failure to the Buyer; and (ii) the Supplier shall provide the Buyer with a reasonable opportunity to correct such failure before performing such additional services.

5. Buyer Data and Security

- A. The Supplier and the Buyer shall comply with their respective security provisions set out in the DPA.

B. The Buyer shall:

- 1. nominate Buyer Users who will have access to the Products and, without limiting the Buyer's liability for any breaches of these Supplier Licence Terms, the Buyer shall be liable for their use, or misuse, of the Products;
- 2. keep, and shall ensure Buyer Users keep confidential any user name and password assigned to them and shall be responsible for protecting and securing

said user names and passwords and preventing, so far as possible, any unauthorized use of the Products;

3. notify the Supplier of any actual or anticipated unauthorized or improper access to or use of the Products reasonably known by Buyer, including but not limited to a Buyer User being or becoming affiliated with a known competitor of the Supplier, as soon as the Buyer becomes aware of this; and
4. the Supplier reserves the right to suspend access to the Products for any Buyer User if the Supplier reasonably believes that the continued use of the Products could result in a disclosure of the Supplier Confidential Information; provided, however, the Supplier shall provide written notice of such suspension to the Buyer as soon as reasonably possible after such suspension.

6. Intellectual Property Rights

- A. All Intellectual Property Rights in the Products produced by the Supplier shall remain the property of the Supplier and/or its licensors.
- B. The Buyer hereby grants to the Supplier during the term of each agreement with the Buyer, a limited, non-exclusive, non-transferrable, non-sublicensable, royalty-free license to access, modify, and otherwise use Buyer Data for the sole purpose of providing the Products and for no other purpose. The Supplier acknowledges that Buyer Data is licensed, not sold, to the Supplier. The Supplier agrees that, as between the Supplier and the Buyer, the Buyer is the sole and exclusive owner of all of the right, title, and interest in and to Buyer Data and any modifications or improvements thereto, and in and to all associated Intellectual Property Rights therein.

7. Indemnity

- A. The Supplier shall defend Buyer and its affiliates, and their directors, officers, employees, and shareholders ("Buyer Indemnified Parties"), from and against any and all demands, suits, claims, actions, liabilities, losses, damages, costs and expenses (including, but not limited to, interest, penalties, reasonable attorneys' fees and other expenses of litigation) and causes of action of whatsoever kind ("collectively "Claim(s)") arising from or incurred by reason of: (i) any infringement or alleged infringement of any Intellectual Property Right of a third party suffered or incurred as a result of or in connection with the development or use of the System and will indemnify and hold harmless the Buyer Indemnified Parties from and against liabilities, losses, damages, costs and expenses (including, but not limited to, interest, penalties, reasonable attorneys' fees and other expenses of litigation) ("Loss") incurred as a result of such Claim.
- B. The Buyer shall not be entitled to the remedy set out in Section 7.A. to the extent that the Loss results from the Buyer's use of the Products other than in accordance with the terms of the Agreement.
- C. The Buyer shall defend the Supplier and its affiliates, and their directors, officers, employees, and shareholders ("Supplier Indemnified Parties") from and

against all Claims arising from or incurred by reason of: (i) the Supplier's use of any material provided by the Buyer or Users for inclusion in the Products and will indemnify and hold harmless Supplier Indemnified Parties from and against any all Losses incurred as a result of such Claim.

- D. The Supplier shall not be entitled to the remedy set out in Section 7.C. to the extent that the Losses that it has incurred or suffered are as a direct result of the Supplier using any material otherwise than in accordance with the terms of the Agreement or Buyer's written instructions (including any policies, procedures or other documentation).
- E. In the event of a claim or demand covered by Section 7, the indemnified party agrees to: (i) give the indemnifying party the sole authority in the defence or settlement (with prior written approval by the indemnified party, which shall not be unreasonably withheld) of any Claim; (ii) provide all reasonable assistance, at the indemnifying party's expense, in any such defence; and (iii) give prompt written notice of and description of each Claim provided, however, that the failure to give such notice shall not relieve the indemnifying party of its obligations hereunder except to the extent that the indemnifying party was actually and materially prejudiced by such failure.

8. Liability

- A. The Supplier and its sub-contractors shall not be liable for the accuracy of data entered into the Products by the Buyer, Buyer Users or Candidates nor for misuse of the Products by the Buyer, Buyer Users or Candidates.
- B. The Buyer acknowledges and accepts that the Products are intended to provide a guide only to the Buyer and Buyer affiliates of the suitability and aptitude of a Candidate and accordingly, the Buyer will be solely responsible for all decisions taken or not taken in respect of a Candidate.

9. Warranties

- A. The Supplier represents and warrants that:
 - 1. it has the right, power and authority, and has taken all action necessary, to execute, deliver and exercise its rights, and perform its obligations, under these Supplier Licence Terms;
 - 2. it is the owner of, or has the authority to license use of, the Products and that no third parties have any rights therein which might cause the Supplier to be unable to provide the Products as contemplated in these Supplier Licence Terms;
 - 3. it will use commercially reasonable efforts to ensure the Products do not contain any computer viruses, worms, software bombs or similar items; and
 - 4. it shall perform its obligations under these Supplier Licence Terms in a professional and workmanlike manner and in accordance with industry standards.

10. AI Terms

A) The Supplier provides the AI Products to the Buyer subject to the provisions of this Section 10, which applies in addition to the other terms of the Supplier Licence Terms. In the event of any conflict between the provisions of this Section 10 and the other terms of the Supplier Licence Terms, the provisions of these AI Terms shall prevail in relation to the AI Products only.

B. Input:

1. The Buyer (or its licensors) own Input provided by the Buyer or Users, ("**Buyer Input**"). The Supplier (or its licensors) own or have the right to use Input provided by the Supplier (or its licensors).
2. The Buyer represents and warrants that it (or its licensors) have obtained all rights, licenses and consents required to permit the Supplier to use Buyer Input within the AI Products using the AI Functionality to create Output. The Buyer is solely responsible for ensuring that all Buyer Input provided to the Supplier complies with all applicable laws.
3. The Buyer grants the Supplier a non-exclusive, worldwide, royalty free, right to permit the Supplier and its AI Providers to use Buyer Input within the AI Products using the AI Functionality for the purpose of generating Output.
4. The Supplier only permits AI Providers to access and use Input exclusively to create Output via the AI Functionality for the Buyer.
5. The Supplier (or its licensors) own or have the right to use any Input provided by the Supplier (or its licensors), ("Supplier Input").
6. The Buyer acknowledges and agrees that the Supplier will use pseudonymised or anonymised Buyer Input and Output for the purposes of improving the AI Products for Supplier customer generally.

C. AI Providers:

1. By using the AI Products, the Buyer acknowledges and agrees to the Supplier's using the AI Providers to provide AI Functionality and create Output.
2. Where AI Products are developed using AI models or systems provided by AI Providers, the Buyer acknowledges and understands that by using the AI Products the Buyer agrees that use of the AI Products is subject to each AI Provider's own terms of service, set out in Appendix 1 – AI Providers.
3. The Supplier only permits its AI Providers to access and use Buyer Input exclusively to create Output via the AI Functionality for use by the Buyer and Users. Buyer Input is not used by AI Providers for any other purposes. Buyer Input is not used by AI Providers for machine learning of their own AI models or systems.

4. Any changes to the AI Providers used after the date that the Buyer is granted access to first start using any AI Products will be notified to the Buyer by email from time to time.

D. Personal Data

1. Where Input includes personal data (or personally identifiable information) of the Buyer or its Users, as defined by applicable data protection laws, the Buyer confirms that it has obtained all relevant consents for the Buyer and Users to permit the Supplier and the AI Providers to process personal data for the purposes of the AI Functionality generating Output in the provision of the AI Products, which includes permission to transfer Input to countries where the AI Providers operate, store, and process the Input.
2. The Buyer warrants that it shall: (i) provide its own privacy policy to Candidates, setting out the nature of this processing by the Supplier and the use of the AI Functionality; and (ii) obtain each Candidate's consent to such use of their personal data by the Supplier; prior to making any Candidate's personal data available for use within the AI Products.
3. Where any AI Provider has access to personal data and proposed change in the AI Providers used shall be notified to the Buyer in accordance with the terms of the Supplier DPA.

E. Output

1. Due to the nature of machine learning, Output will not be unique across all Supplier customers and their users and the Buyer acknowledges that the use of AI Functionality within AI Products may generate the same or similar Output for other clients and their users. Output received by other clients or users of the AI Products is not Buyer Output.
2. The Supplier authorises the Buyer to use Output for their business purposes, as deemed appropriate by the Buyer, and in compliance with all applicable laws.
3. The Supplier and any AI Provider used to provide the AI Functionality within the AI Products, make no representations or warranties of any kind, express or implied, in relation to any Output, including without limitation, the accuracy, availability, suitability, reliability, or Content of the Output. The Buyer is solely responsible for all Output, in particular ensuring that Output complies with all applicable laws and compliance with the provisions of these AI Terms.
4. The Supplier has no liability or responsibility: (i) resulting from the use of, or reliance upon any Output by the Buyer or Users; or (ii) for any errors or omissions contained in the Output or Content.
5. The Output produced is a suggestion designed to assist the Buyer and Users in making decisions related to the operation of their business and the use of the AI Products, as applicable. Using the AI Products to create Output does not replace the need for the Buyer and Users to use human judgement to

decide upon the suitability of the Output before it is published, used or relied upon by the Buyer or Users, where the Output will have a legal or significantly similar impact on an individual's rights.

6. The Buyer and Users must check and evaluate the accuracy of any Output before using it and must not rely on the Supplier to do this.
7. The AI Functionality does not make any automated final decisions. It is always the Buyer or User's responsibility to review the Output and make any final determination of their recruitment decisions. Where the AI Functionality is used for scoring, it provides a suggested evaluation and the Buyer must review any scoring suggestions as the Buyer retains full control and can override any AI generated score to ensure that the final score is always determined by a human being.
8. The Buyer acknowledges and agrees that the Supplier has no control over any use of the Output by the Buyer or Users. Any use of Output is at the Buyer's own risk. Prior to publication or distribution of any Output, the Buyer must disclosure that the Output was generated by AI tools.
9. The Buyer has no responsibility: (i) resulting from the use of, or reliance upon any Output by the Buyer or Users; or (ii) for any errors or omissions contained in Output.
10. The AI Products must not be used for contacting emergency services or obtaining immediate emergency assistance. In the event of an emergency, it is crucial to immediately contact the appropriate emergency services in the Buyer's jurisdiction or seek direct assistance from local authorities. The Buyer acknowledges and agrees that the Supplier shall not be held liable for any consequences, damages, or losses arising from any inability to use the AI Products for emergency communication or for any reliance placed on the AI Products during emergency situations.

F. Employment Law

1. The Buyer acknowledges and agrees that the Supplier is not an employment service, an employment agency, or a recruiting or placement agency. The AI Products are tools that make suggestions to the Buyer and User to assist them in making their own independent employment and/or career decisions. The Buyer must independently evaluate any suggested scores or ranking of Candidates created by the AI Functionality and the Buyer alone is solely responsible for all employment decisions made in relation to Candidates when using any AI Products.

G. Indemnity

1. The Buyer shall, at its own expense, defend or, at their option, settle any claim or suit relating to Input or the Output brought against the Supplier or its AI Providers by a third party on the basis of infringement of their Intellectual Property Rights or other rights in any Buyer Input or Output.

H. Warranties

1. The Buyer represents and warrants that it will not, nor will it authorise anyone on its behalf, including a User, to use the AI Products: (i) to mislead anyone that the Output generated by the AI Products is solely human-generated; (ii) to generate content that is prohibited under the terms of the Agreement or any applicable laws; (iii) to generate content that is unlawful, harmful, threatening, defamatory, obscene, harassing or racially or ethnically offensive, facilitates illegal activity, depicts sexually explicit images, or promotes unlawful violence, discrimination based on race, gender, colour, religious belief, sexual orientation, disability, or is otherwise illegal; (iv) to make automated decisions that may have a detrimental impact on individual rights without appropriate human supervision; (v) for activities which have high risk of economic harm, for adult content, adult industries, dating apps, offering tailored financial advice without a qualified person reviewing the information or to provide health advice, political campaigning or lobbying; (vi) in a way that infringes, misappropriates or violates any of the Supplier's rights or the rights of any third party; (vii) to reverse assemble, reverse compile, decompile, translate or otherwise attempt to discover the source code or underlying components of models, algorithms, and systems of the AI Products (except to the extent such restrictions are contrary to applicable law); (viii) to develop foundation models, other large scale models or AI Products that replicates the AI Products; (ix) to compete with the Supplier or (x) to use any method to extract data from the AI Products, including web scraping, web harvesting, or web data extraction methods.

I. No Warranty

1. The Supplier does not guarantee or warrant any features or qualities of the AI Products and any warranties included in the other terms of the Agreement are explicitly excluded in relation to the AI Products. No warranty or undertaking shall be implied by the Buyer from any description of the AI Products or any other communication.
2. In particular, the Supplier does not warrant that the AI Products will be available uninterrupted, error free or permanently.

J. Limitation of Liability

1. To the maximum extent permitted by law and in addition to the caps on liability set out in the other terms of the Agreement, the Supplier shall not be liable to the Buyer, Users or any third party for any damages arising in connection with: (i) use of, or inability to use, the AI Products; or (ii) any defect in the AI Products; or (iii) use or reliance upon any Output; and (iv) any third party claims relation to Buyer Input. This disclaimer of liability shall apply regardless of the form of action that may be brought against the Supplier, whether in contract or tort including without limitation any action for negligence.
2. Notwithstanding anything to the contrary herein or in the other provisions of the Agreement, under no circumstances shall the Supplier be liable to the Buyer, Users or any other person or entity for any special, incidental, consequential, or

indirect damages, loss of good will or business profits, work stoppage, data loss, computer failure or malfunction, any and all other commercial damages or loss, or exemplary or punitive damages relating to the AI Products.

11. Conflicts

A. In the event of a conflict between these Supplier Licence Terms and the other terms of the documents making up the Agreement, the documents will prevail in the following order:

- Section 10 - AI Terms
- Remainder of the Supplier Licence Terms
- Each Order Form
- The other terms of the Agreement and its schedules

Appendix 1 - AI Providers

The Supplier currently uses the following AI Providers to provide AI Functionality within the AI Products.

- Amazon Bedrock (AWS): <https://aws.amazon.com/service-terms/>
- Anthropic: [Terms of Service](#)
- Mistral: <https://mistral.ai/terms#partner-served-deployment-terms>
- Voiceflow: [Voiceflow Terms of Service](#)

END OF LICENSE TERMS

DATA PROCESSING AGREEMENT (DPA) - For G Cloud 15

This Service Level Agreement is incorporated and forms part of the Supplier Terms

1. Definitions

1.1 Any capitalised term not defined in this DPA shall have the meaning given to it in the Agreement:

- 1.1.1 **"Affiliate"** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with a party, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;
- 1.1.2 **"Agreement"** means the Agreement between the Client and Oleeo for the provision of the Services which this DPA is annexed and incorporates all of the documents referred to in the Agreement;
- 1.1.3 **"Applicable Laws"** has the meaning given in the Agreement;
- 1.1.4 **"Client" means Buyer**
- 1.1.5 **"Client Data" means Buyer Data**
- 1.1.6 **"Client Personal Data"** means any Personal Data Processed by Oleeo or a Subprocessor of Oleeo, on behalf of the Client, pursuant to or in connection with the Agreement (as may be more particularly described in Appendix A) and includes "personally identifiable information", as that term is defined in US State Privacy Laws;
- 1.1.7 **"Client User" means Buyer User**
- 1.1.8 **"DPA"** means this Data Processing Agreement together with its Appendices
- 1.1.9 **"Data Protection Laws"** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom, any amendments, replacements or renewals thereof, applicable to the processing of Personal Data, including where applicable the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, the EU GDPR, the UK GDPR, the UK Data Protection Act 2018, the FADP, US State Privacy Laws and any applicable national implementing laws, regulations and secondary legislation relating to the processing of the Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426);
- 1.1.10 **"EEA"** means the European Economic Area;
- 1.1.11 **"EU GDPR"** means Regulation (EU) 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, (General Data Protection Regulation);
- 1.1.12 **"FADP"** means the Swiss Federal Act on Data Protection of the 1st of September 2023, and as amended from time to time;
- 1.1.13 **"Oleeo" means Supplier**
- 1.1.14 **"Restricted Transfer"** means (where the context so permits):
 - (a) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and

- (b) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and
 - (c) a transfer of Personal Data via the Services from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission.
- 1.1.15 **"Services"** means all services, products, software applications and any other activities supplied to or carried out by or on behalf of Oleeo for the Client pursuant to the Agreement;
- 1.1.16 **"SCCs"** means:
 - (a) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries published at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN>, ("**EU SCCs**"); and
 - (b) where the UK GDPR applies the international data transfer addendum to the EU SCCs adopted pursuant to Article 46(2)(c) of the UK GDPR and published at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>, as may be amended or replaced, ("**UK SCCs**"); and
 - (c) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority; ("**Swiss SCCs**")
 As they may be amended, superseded or replaced from time to time.
- 1.1.17 **"Subprocessor"** means any person (including any third party and any Oleeo Affiliate, appointed directly or indirectly by Oleeo to Process Client Personal Data on behalf of the Client in connection with the Agreement pursuant to this DPA;
- 1.1.18 **"UK GDPR"** means the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018;
- 1.1.19 **"US State Privacy Laws"** means the following US state data protection or privacy laws and regulations applicable to the party's Processing of Personal Data: California Consumer Privacy Act (**CCPA**) as amended by the California Privacy Rights Act (**CPRA**), Virginia Consumer Data Protection Act (**VCDPA**), Colorado Privacy Act (**CPA**), Connecticut Data Privacy Act (**CTDPA**), and Utah Consumer Privacy Act (**UCPA**) and the Connecticut Data Privacy Act (**CTDPA**), the Montana Consumer Data Privacy Act (**MCDPA**), Consumer Data Protection (**Iowa CDPA**), the Delaware Personal Data Privacy Act (**DPDPA**), the Nebraska Data Privacy Act (**NDPA**), the New Hampshire Expectation of Privacy Act (**NHPA**) and the New Jersey Act Concerning Online Services, Consumers, and Personal Data (**NJDPA**), in each case as may be amended or superseded from time to time in each case as may be amended or superseded from time to time.
- 1.2 The terms **"Controller"**, **"Data Subject"**, **"Member State"**, **"Personal Data"**, **"Personal Data Breach"**, **"Processing"**, **"Processor"**, **"pseudonymisation"** and **"Supervisory Authority"** shall have the same meaning as in applicable Data Protection Law, and their cognate terms shall be construed accordingly.
- 1.3 The word **"include"** shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Arrangement between the Parties

- 2.1 Oleeo has agreed to provide the Services to the Client in accordance with the terms of the Agreement. In providing the Services, Oleeo shall process Client Data on behalf of the Client. Client Data will include Client Personal Data. Oleeo will process and protect Client Personal Data in accordance with the terms of this DPA.

- 2.2 In providing the Services to the Client pursuant to the terms of the Agreement, Oleeo shall process Client Personal Data only to the extent necessary to provide the Services in accordance with the terms of the Agreement, this DPA and the Client's instructions documented in the Agreement and this DPA, as updated from time to time.
- 2.3 Each Party shall Process Personal Data which is professional contact data, in relation to the other party's representatives (in its capacity as a Controller) to administer the Agreement. Each Party shall Process the other Party's contact data for the purposes set out in this paragraph in accordance with that Party's relevant privacy policy. Each Party may be required to share the other Party's contact data with its Affiliates and other relevant parties, within or outside the country of origin, to administer the Agreement but in doing so, each Party will ensure that the sharing and use of the contact data complies with applicable Data Protection Laws.
- 2.4 The Client represents and warrants that all Affiliates of the Client who use the Services shall comply with the obligations of the Client set out in this DPA.
- 2.5 The Client acknowledges and agrees that some instructions from the Client including Oleeo assisting with audits, inspections, data privacy impact assessments or providing any assistance under this DPA, may result in additional fees. In such case Oleeo shall notify the Client of its fees for providing such assistance in advance and shall be entitled to charge the Client for its reasonable costs and expenses in providing such assistance, unless agreed otherwise in writing.

3. Processing of Client Personal Data

- 3.1 Oleeo shall:
 - 3.1.1 comply with its obligations under all applicable Data Protection Laws in the Processing of Client Personal Data;
 - 3.1.2 not Process Client Personal Data other than on the Client's documented instructions unless required to do so by Applicable Law in which case Oleeo shall, to the extent permitted by law, inform the Client of that legal requirement before the relevant Processing of that Client Personal Data.
- 3.2 The Client instructs Oleeo (and authorises Oleeo to instruct each Subprocessor (where applicable)) to Process Client Personal Data and transfer Client Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Agreement.
- 3.3 If Oleeo becomes aware it cannot process Personal Data in accordance with the Client's instructions, including due to a legal requirement or if such instructions infringe applicable Data Protection Laws Oleeo will, to the extent permitted by Applicable Law, promptly notify the Client and, where necessary, cease all processing (save for storing and maintaining the security of such Personal Data) until the Client issues new instructions with which Oleeo can comply. Oleeo will not be liable for any failure to perform the Services under the Agreement until the Client issues revised and lawful instructions relating to the processing.
- 3.4 Appendix A, to this Schedule 1 sets out certain information regarding Oleeo's Processing of the Client Personal Data as required by Article 28(3) of the EU GDPR. The Client may make reasonable amendments to Appendix A by written notice to Oleeo from time to time as the Client reasonably considers necessary to meet those requirements. Nothing in Appendix A (including as amended pursuant to this paragraph 3.4) confers any right or imposes any obligation on any Party to this Schedule.
- 3.5 Oleeo and the Client shall take steps to ensure that any natural person acting under the authority of the Oleeo or the Client who has access to Client Personal Data does not process Client Personal Data except on the instructions from the Client, unless required to do so by any Data Protection Law.
- 3.6 Client shall be solely responsible for:
 - 3.6.1 The accuracy, quality and legality and the means by which the Client acquired the Personal Data;
 - 3.6.2 Complying with its obligations under all applicable Data Protection Laws for the collection and use of Personal Data, including obtaining any necessary consents, particularly for Client's marketing purposes;

- 3.6.3 Ensuring that the Client has the right to transfer or provide access to the Client Personal Data in accordance with the terms of the Agreement and this DPA; and
- 3.6.4 Ensuring that the Clients instructions to Oleeo regarding the processing of Personal Data comply with all Applicable Laws and Data Protection Laws.
- 3.6.5 The Client agrees to inform Oleeo without undue delay if it is not able to comply with the above or any applicable Data Protection Laws.

4. Confidentiality

- 4.1 Oleeo shall ensure that all employees, agents, officers and contractors involved in the handling of Client Personal Data:
 - 4.1.1 Are aware of the confidential nature of the Client Personal Data and are contractually bound to keep the Client Personal Data confidential;
 - 4.1.2 Have received appropriate training on their responsibilities as a data processor; and
 - 4.1.3 Are bound by the terms of this DPA.

5. Security

- 5.1 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, Oleeo shall, in relation to the Client Personal Data, implement appropriate technical and organisational measures to protect Client Personal Data. Oleeo shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access, appropriate to the risk, which may include:
 - 5.1.1 the pseudonymisation and encryption of the Client Personal Data;
 - 5.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - 5.1.3 the ability to restore the availability and access to the Client Personal Data in a timely manner in the event of a physical or technical incident;
 - 5.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- 5.2 In assessing the appropriate level of security in paragraph 5.1, Oleeo shall take account of the risks that are presented by Processing, in particular, from a Personal Data Breach and include, as appropriate, the measures referred to in Article 32(1) of the UK GDPR, including the measures set out in Annex B of this DPA ("**Security Measures**") The Client is responsible for independently determining whether the data security provided by Oleeo adequately meets the Clients' obligations under the Data Protection Laws.
- 5.3 The technical and organisational measures detailed in Appendix B of this DPA shall at all times be adhered to as a minimum security standard. The Client accepts and agrees that the technical and organisational measures are subject to development and review and that Oleeo may use alternative suitable measures to those detailed in the attachments to this DPA, provided such measures are at least equivalent to the technical and organisational measures set out in Appendix B and appropriate pursuant to Oleeo's obligations in clauses 5.1 and 5.2 above.
- 5.4 Oleeo confirms that it and/or its Affiliate(s) have appointed a data protection officer where such appointment is required by Data Protection Laws. The appointed data protection officer may be contacted by email at: dpo@oleeo.com.
- 5.5 The Client shall implement appropriate technical and organisational measures to protect Personal Data, taking into account, the state of the art; the costs of implementation; the nature, scope, context and purposes of processing; and the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Client shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

6. Subprocessing

- 6.1 The Client agrees that Oleeo may engage Subprocessors to assist in providing the Services. Oleeo has, at the date of this Agreement, appointed the subcontractors and its Affiliates listed [here](#) as its Subprocessors. Some Subprocessors will apply by default and others apply only if the Client opts-in to the Services that they provide.
- 6.2 The Client authorises Oleeo to appoint (and permit each Subprocessor appointed in accordance with this paragraph 6 to appoint) Subprocessors in accordance with this paragraph 6 and any restrictions in the Agreement.
- 6.3 If Oleeo adds or replaces any Subprocessors used in the provision of the Services, it shall give the Client 30 days prior notice by email of the proposed appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor, unless a Subprocessor needs to be added or replaced as a matter of urgency e.g. for security reasons in which case a shorter and reasonable notice period may be given. If, within thirty days of receipt of that notice, the Client notifies Oleeo in writing of any objections, acting reasonably, to the proposed appointment:
- 6.3.1 Oleeo shall work with the Client in good faith to consider alternatives to any obligations;
 - 6.3.2 Oleeo shall not appoint (or disclose any Client Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by the Client and the Client has been provided with a reasonable written explanation of the steps taken; and
 - 6.3.3 Where an alternative solution cannot be found, notwithstanding anything in the Agreement to the contrary, the Parties, acting reasonably, shall seek to agree a Subprocessor which is acceptable to both of them and if none can be agreed, Oleeo shall appoint a new Subprocessor or permit the Client to suspend or terminate the affected Services in accordance with the termination provisions of this Agreement without liability to either Party, save for any fees incurred by the Client prior to suspension or termination.
 - 6.3.4 If the Client does not raise any objection to a proposed Subprocessor within the 30 day period set out in clause 6.3.3 the new Subprocessor will be deemed to have been agreed to on expiry of such 30 day notice period.
- 6.4 With respect to each Subprocessor, Oleeo shall:
- 6.4.1 before the Subprocessor first Processes Client Personal Data, carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Client Personal Data required by the Agreement;
 - 6.4.2 ensure that the arrangement between Oleeo, and the Subprocessor, is governed by a written contract including terms which impose substantively the same obligations on the Subprocessor as this DPA imposes on Oleeo;
 - 6.4.3 if that arrangement involves a Restricted Transfer, Oleeo will ensure that such Subprocessors: (i) are located in a third country or territory recognised by the EU Commission or a Supervisory Authority, as applicable, to have an adequate level of protection; or (ii) have entered into the applicable SCCs with Oleeo; or (iii) have other legally recognised appropriate safeguards in place; necessary to ensure the transfer is in compliance with the applicable Data Protection Laws ;
- 6.5 Oleeo shall ensure, to the extent applicable to the nature of the services provided by the Subprocessors, that each Subprocessor performs the obligations under paragraphs 3.2, 4, 5, 7.1, 8.2, 10 and 11.1, as they apply to Processing of Client Personal Data carried out by that Subprocessor, as if it were Party to this Schedule in place of Oleeo.
- 6.6 Oleeo shall remain responsible for each Subprocessor's compliance with the obligations set out in this clause 6 above and for acts and omissions of such Subprocessor that causes any breach of this DPA.

7. Restricted Transfers

- 7.1 The Parties agree that, when a transfer of Client Personal Data occurs between the Client and Oleeo or from Oleeo to a Subprocessor which is a Restricted Transfer, it shall be subject to the applicable SCCs.

- 7.2 The Parties agree that the EU SCCs shall apply to Restricted Transfers from the EEA. The EU SCCs shall be deemed entered into (and incorporated into this DPA by reference) and completed as follows:
- 7.2.1 Module Two (Controller to Processor) shall apply where the Client is a Controller of Client Personal Data and Oleeo is processing Client Personal Data;
 - 7.2.2 Module Three (Processor to Processor) shall apply where Oleeo is a Processor of Client Personal Data and Oleeo uses a Sub-processor to process the Client Personal Data;
 - 7.2.3 Module Four (Processor to Controller) shall apply where Oleeo is processing Client Personal Data and the Client is not subject to the EU GDPR or UK GDPR;
 - 7.2.4 In Clause 7 of the EU SCCs, the optional docking clause shall not apply;
 - 7.2.5 In Clause 9 of the EU SCCs, Option 2 applies, and the time period for giving notice of Subprocessor changes shall be 30 days;
 - 7.2.6 In Clause 11 of the EU SCCs, the optional language shall not apply;
 - 7.2.7 In Clause 17 of the EU SCCs, Option 1 applies and the EU SCCs shall be governed by Irish law;
 - 7.2.8 In Clause 18(b) of the EU SCCs, disputes shall be resolved by the courts of Ireland;
 - 7.2.9 Annex I of the EU SCCs shall be deemed completed with the information set out in Appendix A of this DPA;
 - 7.2.10 Annex II of the EU SCCs shall be deemed completed with the information set out in Appendix B of this DPA.
- 7.3 The Parties agree that the EU SCCs as amended in clause 7.2 above, shall be adjusted as set out below where the FADP applies to any Restricted Transfer:
- 7.3.1 The Swiss Federal Data Protection and Information Commissioner ("FDPIC") shall be the sole Supervisory Authority for Restricted Transfers exclusively subject to the FADP;
 - 7.3.2 Restricted Transfers subject to both the FADP and the EU GDPR, shall be dealt with by the EU Supervisory Authority named in Appendix A of this DPA;
 - 7.3.3 The term 'member state' must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;
 - 7.3.4 Where Restricted Transfers are exclusively subject to the FADP, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP;
 - 7.3.5 Where Restricted Transfers are subject to both the FADP and the EU GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP insofar as the Restricted Transfers are subject to the FADP;
- 7.4 The Parties agree that the UK SCCs shall apply to Restricted Transfers from the UK and the UK SCCs shall be deemed entered into (and incorporated into this DPA by reference), completed as follows:
- 7.4.1 Table 1 of the UK SCCs shall be deemed completed with the information set out in Appendix A of this DPA;
 - 7.4.2 Table 2 of the UK SCCs shall be deemed completed with the information set out in clauses 7.2.1 – 7.2.8 of this DPA;
 - 7.4.3 Table 3 of the UK SCCs shall be deemed completed with the information set out in Appendices A and B of this DPA; and
 - 7.4.4 Either Party may end the UK SCCs as set out in clause 19 of the UK SCCs.
- 7.5 In case of any changes to the EU SCCs or UK SCCs, the Parties shall negotiate in good faith necessary amendments to the DPA and the Agreement to ensure compliance with applicable Data Protection Laws.
- 7.6 In the event that any provision of this DPA contradicts directly or indirectly any SCCs, the provisions of the applicable SCCs shall prevail over the terms of this DPA.
- 7.7 Should countries other than those in the EEA, UK or Switzerland adopt cross-border data transfer clauses similar to the SCCs, the Client and Oleeo agree to execute such clauses when necessary.

8. Data Subject Access Rights

- 8.1 Taking into account the nature of the Processing and the information available to Oleeo, Oleeo shall assist the Client by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Client's obligations, to respond to requests to exercise Data Subject rights under the Data Protection Laws in respect of the processing of Client Personal Data.
- 8.2 Oleeo shall:
- 8.2.1 promptly notify the Client and advise the Data Subject to refer their request to the Client if Oleeo receives a request from a Data Subject under any Data Protection Law in respect of Client Personal Data (and in such case the Client shall be solely responsible for responding to such Data Subject request);
 - 8.2.2 where Oleeo or any Subprocessor receives a request from any government of any country (or anybody with delegated authority for any of them) or any other third Party for access to any Client Personal Data ("Disclosure Request"), Oleeo shall, where able, notify the Client immediately and provide all available information (at that point or as it is available);
 - 8.2.3 if Oleeo or its Subprocessor is prevented by law from notifying the Client, Oleeo shall seek to obtain a waiver to such prohibition. In any event, Oleeo or its Subprocessor shall review the Disclosure Request and exhaust all remedies to challenge it if Oleeo concludes there are grounds to do so, document its assessment, challenge it, where permitted, make this information available to the Client and where mandated to disclose the Client Personal data, only provide the minimum amount of information possible based on a reasonable interpretation of the Disclosure Request; and
 - 8.2.4 Oleeo shall provide reasonable assistance to the Client to respond to any Data Subject Requests or requests from data protection authorities relating to the processing of Personal Data under this Agreement subject to the Client reimbursing Oleeo for the commercially reasonable costs of providing such assistance.

9. Personal Data Breach

- 9.1 Oleeo shall notify the Client without undue delay (and no later than twenty-four (24) hours) after Oleeo or any Subprocessor becomes aware of a Personal Data Breach affecting Client Personal Data, providing the Client with relevant information to allow the Client to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
- 9.2 In the event of a Personal Data Breach, Oleeo shall implement any measures reasonably necessary to restore the security of the compromised Client Personal Data and mitigate any material adverse effects of such Personal Data Breach.
- 9.3 In the event of a Personal data Breach, Oleeo shall co-operate with the Client and take such reasonable commercial steps as are directed by the Client to assist in the investigation, mitigation and remediation of each such Personal Data Breach, including any notification needed to the Supervisory Authority and affected Data Subjects, if the Client is required to do so under Data Protection Laws.

10. Data Protection Impact Assessment and Prior Consultation

Oleo shall provide reasonable assistance to the Client, at the Client's cost, to the extent that the required information is reasonably available to Oleeo and is not otherwise accessible to the Client, with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Client reasonably considers to be required of itself by Data Protection Law, in each case solely in relation to Processing of Client Personal Data.

11. Deletion or return of Client Personal Data

- 11.1 Subject to paragraphs 11.2 and 11.3, Oleeo shall, and shall procure that any Subprocessor shall, following the cessation of any Services involving the Processing of Client Personal Data (the "**Cessation Date**"), promptly delete and procure the deletion of all copies of Client Personal Data.

- 11.2 Subject to paragraph 11.3, the Client may in its absolute discretion by written notice to Oleeo, require Oleeo to (a) return a complete copy of all Client Personal Data to the Client by secure file transfer at the Client's cost; and (b) delete and procure the deletion of all other copies of the Client Personal Data Processed by Oleeo.
- 11.3 Oleeo may retain Client Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by that law and always provided that Oleeo shall ensure the confidentiality of all such Client Personal Data and shall ensure that such Client Personal Data is only Processed as necessary for the purpose(s) specified in the Agreement and for the duration of the Agreement.
- 11.4 If the Client requests, Oleeo shall provide written certification to the Client that Oleeo has fully complied with this paragraph 11.

12. Audit rights

- 12.1 Subject to paragraphs 12.2 and 12.3, Oleeo shall make available to the Client all information reasonably necessary to demonstrate compliance with Oleeo's Processing obligations, and shall allow for and contribute to audits, including inspections by the Client or an independent auditor mandated by the Client (at the Client's cost) in relation to the Processing of the Client Personal Data by Oleeo.
- 12.2 Information and audit rights of the Client only arise under paragraph 12.1 to the extent that this Agreement does not otherwise give it information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, clause 8.3 Module Four of the SCCs).
- 12.3 The Client shall give Oleeo reasonable notice of any audit or inspection to be conducted under paragraph 12.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to Oleeo's premises, equipment, personnel and business while the Client or auditor's personnel are on those premises in the course of such an audit or inspection. Oleeo need not give access to its premises for the purposes of such an audit or inspection:
 - 12.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;
 - 12.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Client has given notice to Oleeo before attendance begins outside of those hours; or
 - 12.3.3 for the purposes of more than one audit or inspection, in respect of Oleeo, in any calendar year, except for any additional audits or inspections which:
 - (a) the Client reasonably considers necessary because of genuine concerns as to Oleeo's compliance with this DPA; or
 - (b) the Client is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory; and
 - (c) where the Client has identified its concerns or the relevant requirement or request in its written notice to Oleeo of the audit or inspection.

13. Liability

- 13.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA or a Party's obligations under applicable Data Protection Law.
- 13.2 The Parties agree that the Client shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Client itself.
- 13.3 The Parties agree that Oleeo shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Subprocessors to the same extent Oleeo would be liable if performing the services of each Subprocessor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

- 13.4 Subject to the financial caps on liability set out in the Agreement, each Party shall be liable to the other for any damages it causes to the other Party by breach of its obligations under this DPA or applicable Data Protection Law provided that it is evidenced not to have complied with its respective obligations under applicable Data Protection Laws or under this DPA.
- 13.5 Neither Party shall be entitled to recover more than once in respect of the same loss.

14. Term and Termination

- 14.1 Oleeo shall only process Client Personal Data for the term of this DPA. The term of this DPA shall commence on the effective date of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

15. Deletion and Return of Personal Data

- 15.1 Oleeo shall at the choice of the Customer, upon receipt of a written request received within 30 days of the end of the provision of the Services, delete or return Client Personal Data to the Client.

16. Order of precedence

- 16.1 Nothing in this DPA reduces Oleeo's obligations under the Agreement in relation to the protection of Personal Data or permits the Processing of Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the SCCs, the SCCs shall prevail.
- 16.2 Subject to paragraph 17.2, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Agreement and (except where explicitly agreed otherwise in writing and signed on behalf of the Parties) any agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

17. General

- 17.1 The Client shall notify Oleeo within a reasonable time, of any changes to any Applicable Law which may affect the contractual duties of Oleeo under this DPA. Oleeo shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If Oleeo is unable to accommodate necessary changes, the Client may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.
- 17.2 The Parties and, where applicable, their representatives, shall cooperate, on request, with a Supervisory Authority in the performance of their respective obligations under this DPA and Data Protection Law.
- 17.3 This DPA sets out the entire understanding of the Parties with regards to the subject matter herein.
- 17.4 Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.
- 17.5 Subject to any provision of the SCCs to the contrary, this DPA shall be governed by the laws of England and Wales. The courts of England shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.
- 17.6 The Parties agree that this DPA is incorporated into and governed by the terms of the Agreement.

Appendix A

List of Parties, Description of Processing and Transfer of Personal Data, Competent Supervisory Authority

A. LIST OF PARTIES

The Exporter: [Not Applicable if the Customer is based only in the UK]

means the Client.	
Address:	As set out for the Client in the Agreement.
Contact person's name, position and contact details:	As provided by the Client in its account and used for notification and invoicing purposes.
Activities relevant to the data transferred under the SCCs:	Use of the Services for the purposes of recruitment and recruiting-related purposes.
Signature and date:	By entering into the Agreement, the Exporter is deemed to have signed the SCCs incorporated into this DPA including its Appendices, as of the date of the Agreement.
Role:	Data Controller.
Name of Representative (if applicable):	Any UK or EU representative named in the Exporter's privacy policy.

The Importer:

means Oleeo Limited	
Address:	5-7 Bridgeworks, The Crescent, Wimbledon, SW19 8DR, United Kingdom.
Contact details:	dpo@oleeo.com

Activities relevant to the data transferred under the SCCs:	The provision of cloud computing solutions to the Exporter under which the Importer processes Personal Data upon the instructions of the Exporter in accordance with the terms of the Agreement.
Signature and date:	By entering into the Agreement, the Importer is deemed to have signed the SCCs, incorporated into this DPA, including its Appendices, as of the date of the Agreement.
Role:	Data Processor.

B. DESCRIPTION OF PROCESSING AND TRANSFERS - Client to review and where this needs editing to include an up to date table within Schedule 7 of the Agreement

Description	Details
Categories of Data Subjects	Employees, agents, advisors, consultants, freelancers of the Controller (who are natural persons). Client Users, Affiliates and other participants authorised by the Controller to access or use the Services in accordance with the terms of the Agreement. Candidates. Other individuals to the extent identifiable in the context of emails of their attachments or in archiving content.
Categories of Personal Data	During the recruitment process Data Subjects may be required to provide the following types of data: Personal Details First name, middle name and surname, e-mail addresses, home postal address, phone numbers. Screening/Selection Information CV / Resume, education results, work experience, significant achievements, etc. Some of this information may include enough information to personally identify a Candidate e.g., Data Subject's CV/Resume. Evaluation Data Information provided by other people involved in the recruitment process about a Candidate's suitability for employment and status within the recruitment process. User feedback on the recruitment process Optional information consisting of feedback on the recruitment process. Special Requirements

	Optional information provided by Candidates e.g., medical needs, dietary requirements, disability, dyslexia, study abroad. Candidate Contractual Information Information provided by Candidates which is required for final contract (in addition to Personal Details). Includes acceptance of offer. Other Contractual Information Information added by the employer in order to draw up a contract e.g., salary, job title, hours. On-Boarding Information Additional information supplied by the Candidate in order to complete the hiring process and may include bank details, proof of right to work, next of kin, etc. Equal Employment Opportunity (EEO) Information Gender, Race, Religion, Veteran, Disability, or other diversity information Other Information collected from all Data Subjects: Unique identifiers such as username, account number or password IP address Personal Data derived from a user's use of the Services such as records and business intelligence information Meta data including sent, to, from, date, time, subject, which may include Personal Data. Geolocation based upon IP address. File attachments that may contain Personal Data. Survey, feedback and assessment messages. Information offered by users of the Services as part of support enquiries. Other data added by the Data Controller from time to time.
Sensitive Data	Personal Data transferred includes but is not limited to the following special categories of Personal Data: • Personal Data revealing racial or ethnic origin • political opinions, • religious or philosophical beliefs • trade union membership • the processing of genetic data • biometric data for the purpose of uniquely identifying a natural person • data concerning health or data concerning a natural person's sex life or sexual orientation • personal data relating to criminal convictions and offences

The frequency of the processing and transfer	Continuous basis for the duration of the Agreement.
Nature of the processing	Processing operations include but are not limited to: 1. Personal Contact data is used to communicate with Candidates and employees during the recruitment process. 2. Screening/Selection data is used to decide on Candidate suitability for jobs which are applied to, or to identify jobs for which Candidates may be more suitable. Screening may be manual or automatic or a combination of both. 3. Evaluation data is used to record assessment of Candidate suitability for jobs that the Candidate is being considered for, including status within the recruitment process. 4. Candidate feedback and application source data is used to improve the recruitment process. 5. Special Requirements data is used to make accommodation in the recruitment process for any needs participants may have. 6. Candidate Contractual Information and Other Contractual Information is used to compile contractual documentation (e.g. job offer and contract) and to record the contract. Candidate data may also be transferred to other systems that are under the control of the data controller, data processor and subcontractors (e.g., payroll systems, reporting tools). 7. On-Boarding Information is used to prepare for new hires starting work including setting up payroll information, benefits, and proof of right to work, including the transfer of information to other systems and subcontractors e.g., payroll systems, background checking agencies. 8. EEO Information is used to monitor the recruitment process to ensure recruitment practices are fair. 9. Data is used as part of aggregate data used by decision analytics, algorithms and reports to provide analysis, insights and predictions to help improve recruitment and drive efficiencies. Aggregated insights, analysis, and learnings are shared completely anonymised. In carrying out the above, the data is processed as follows: • Collected via web forms and received by email from Candidates, employees and subcontractors (such as recruitment agencies) • Stored in a server farm • Processed by computer automatically including: performing calculations; evaluating information and recording results; reformatting information; analysing and the creation of algorithms, insights and predictions; • Re-presented, transferred and communicated via web pages, email, text and file transfers • Erased and destroyed

	Nature and purposes of the processing for Parsing Services (where used) 1. Data from a Candidate and or employee cv for the purposes of parsing into a Candidate's application record or removing an element (such as name) from a cv and representing the cv. 2. Data from the Candidate's social media profile for the purposes of inclusion in the Candidate's application record. 3. Data is normalised and enriched in order to standardise (fit into drop down lists), analyse, report on and match to jobs. 4. Parsing, normalisation and enrichment processing is carried on by software provided by the Subprocessor. In carrying out the above, the data is processed as follows: • Received via API requested from Oleeo and the Client has given Oleeo permission to use Subprocessors. • A data subject's CV or social profile is passed to the Subprocessor by Oleeo, in this instance Parsing technology is hosted by the Subprocessor. • The output of the parsing and/or the data subjects CV is passed to the software provided by the Subprocessor hosted by Oleeo but accessed and maintained from time-to-time by the Subprocessor • The CV or social profile are parsed into separate fields and enriched and normalised by this software, and the resulting data passed back to and stored & processed by Oleeo. In the event where Oleeo hosts the Parsing technology then the following applies: • A data subject's CV or social profile is passed to software provided by the Subprocessor (Subprocessor Software) hosted by Oleeo but accessed and maintained from time-to-time by the Subprocessor for the purposes of updating and maintenance. • The CV or social profile are parsed into separate fields and enriched and normalised by this software, and the resulting data passed back to and stored & processed by Oleeo. • The CV or social profile are not stored by the Subprocessor Software. Where Client wishes Oleeo to send data to third parties which provide additional services to the Client, e.g., HR, payroll integration, assessment provider services. Where AI functionality to match candidates in a talent pool to jobs is used, CV/Applications & Jobs (input) are fed into an algorithm. Skills (output) are extracted from CV/apps & Jobs and are tagged
--	---

	to the CV or Job. A Job's skills tags are fed into a search window, where they are adjusted by a recruiter. These skills are fed into a second algorithm that ranks the set of skills associated with each CV, thus ranking CVs. Where AI functionality to allow a candidate to search for jobs using their CV/Resume is used, CV/Applications & Jobs (input) are fed into an Algorithm. Skills (output) are extracted from CV/apps & Jobs and are tagged to the CV or Job. A candidate's skills tags are fed into a search window, where they are adjusted by the candidate. These skills are fed into a second algorithm that ranks the set of skills associated with each job, thus ranking jobs.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	The Client may specify the period of time for which Personal Data may be retained. Unless agreed otherwise in writing, as per the above, Personal Data will be retained for the duration of the Agreement, and the provisions of the "Plan for return and destruction" set out below.
Plan for return and destruction of the data once the processing is complete	Controller may download data from Processor's systems and request the return of Personal Data provided outside of the Processor's systems. Data shall be deleted in accordance with the following: (i) Subject to (ii), Client may in its absolute discretion by written notice to Oleeo require Oleeo to (a) return a complete copy of all Client Personal Data to Client by secure file transfer at Client's cost; and (b) delete and procure the deletion of all other copies of Client Personal Data processed by Oleeo or any Subprocessor; (ii) Oleeo or any Subprocessor may retain Client Personal Data to the extent required by Applicable Law and only to the extent and for such period as required by that law and always provided that Oleeo shall ensure the confidentiality of all such Client Personal Data and shall ensure that such Client Personal Data is only processed as necessary for the purpose(s) specified in the Applicable Law requiring its storage and for no other purpose. Upon request, the Processor's system can be configured to auto-anonymise or auto-delete data after a period specified by the Client in the vacancy. (Additional Costs apply). Alternatively, deletion can be achieved by the Client through a manually audited process at a period specified by the Client. Where Parsing is used by the Client and the Parsing technology is hosted by a Subprocessor, the data held by the Subprocessor

	will be erased within a maximum of 48 hours further to completion of processing.
For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:	The Subprocessor list published in Appendix C of this DPA sets out the Personal Data processed by each or and the services provided by each Subprocessor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies (e.g. in accordance with Clause 13 of the SCCs)	Where the EU GDPR applies, the Irish Data Protection Authority - Data Protection Commission, (DPC). Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO). Where the FADP applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).
--	---

Appendix B

Security Policy

Technical and Organisational Security Measures (Including Technical and Organisational Measures to Ensure the Security of Data)

Below is a description of the technical and organisational measures implemented by Oleeo (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Where applicable this Appendix B will serve as Annex II to the SCCs.

Measure	Description
Measures of pseudonymisation and encryption of Personal Data	For the purpose of transfer control, an encryption technology is used (e.g. remote access to the Oleeo network via two factor VPN tunnel and full disk encryption). The suitability of an encryption technology is measured against the protective purpose. The Controller's archived data is encrypted at rest using FIPS 140-2 compliant AES256 bit encryption Data in transit is protected by Transport Layer Security ("TLS") 1.2 or above ciphers
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept. In accordance to the "least privilege" and "need-to-know" principles, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person. To maintain data access control, encryption technology is applied to the Personal Data itself where deemed appropriate to protect sensitive data based on risk.
Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident	The Processor maintains redundancy throughout its IT infrastructure in order to minimize the lack of availability to or loss of data. Backups are maintained daily in accordance with our backup procedures. The Processor maintains a disaster recovery policy and at least once per calendar year practice executing the policy.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	The Processor conducts multiple internal audits based on various frameworks (CIS, NIST etc.). The Processor obtains an external security and compliance audit once per calendar year.

Measures for user identification and authorisation	Oleeo offers Single Sign on, Multi-factor Authentication and username and password. Oleeo can also offer IP address restriction. Access to sensitive data is based on need to know, based on least privilege, managed through configuration. Access to each Clients' environment can be limited to configuration or production environment only or a combination of both. Access will be based on each Clients' requirements
Measures for the protection of data during transmission	Data in transit is protected by Transport Layer Security ("TLS") v1.2 or above or Secure Shell Protocol (SSH).
Measures for the protection of data during storage	The Controller's archived data is encrypted at rest using AES256 bit encryption and data in transit is protected by Transport Layer Security ("TLS").
Measures for ensuring physical security of locations at which Personal Data are processed	Due to their respective security requirements, business premises and facilities are subdivided into different security zones with different access authorisations. Third party data centres are monitored by security personnel and have 24/7 CCTV coverage. Access for employees is only possible with an encoded ID with a photo on it, biometrics and key pin pad entry. All other persons have access only after having registered before (e.g. at the main entrance). Access to special security areas for remote maintenance is additionally protected by a separate access area. The constructional and substantive security standards comply with the security requirements for data centres.
Measures for ensuring events logging	All requests and request processing are logged therefore it is possible to review retroactively whether and by whom Personal Data was entered, altered or deleted.
Measures for ensuring system configuration, including default configuration	Oleeo's base solution includes default configuration that has been through robust Quality Control measures. Oleeo's Quality Control processes are ISO9001 certified. From the point of implementation onwards, Oleeo ensures client specific system configuration through a process of quality control, managed by Oleeo and/or the Client dependent on whether the Client is managing their own System Configuration. System configuration is pushed from the Configuration environment to the Production environment further to testing by the Client and or Oleeo as appropriate.

Measures for internal IT and IT security governance and management	Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems. The Controller's Personal Data is stored in a way that logically separates it from other customer data. Data is stored in separate databases and file system directories secured by application access control. Application access control prevents cross-querying more than one individual client system.
Measures for certification/assurance of processes and products	The Processor is ISO 27001 certified and will continue to maintain these certifications for the term of the Agreement. The technical and organisational measures defined herein are implemented on the basis of the international standard ISO 27001. The Processor shall maintain controls materially as protective as those provided in the ISO 27001. The Processor utilises third party data centres that maintain current ISO 27001 certifications. The Processor will not utilise third party data centres that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations. Upon the Controller's written request (no more than once in any 12 month period), the Processor shall provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Services). Any audit report submitted to the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties The Processor is Cyber Essentials and Cyber Essentials Plus certified and will continue to maintain these certifications for the term of the Agreement.
Measures for ensuring data minimisation	Oleeo provides manual and/or automated deletion facilities for the controller to manage their deletion requirements in line with their data minimisation policy.
Measures for ensuring data quality	The Processor does not assess the quality of the data provided by the Controller or Users. The Processor provides reporting tools within our product to help the Controller understand and validate the data that is stored.
Measures for ensuring limited data retention	Oleeo provides manual and/or automated deletion facilities for the controller to manage their deletion requirements in line with their data minimisation policy.

Measures for ensuring accountability	The Processor internally reviews its information security policies semi-annually to ensure they are still relevant and are being followed. All employees that handle sensitive data must acknowledge the information security policies. These employees are assessed on information security policies once per year. A disciplinary policy is in place for employees that do not adhere to information security policies.
Measures for allowing data portability and ensuring erasure	The Services have built-in tools that allow the Controller to export and permanently erase data.
Measures to be taken by the (Sub-) processor to be able to provide assistance to the Controller (and, for transfers from a Processor to a Sub-processor, to the Data Exporter).	The transfer of Personal Data to a third party (e.g. customers, subcontractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred outside the EEA, the Processor provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the EU SCCs.



Appendix C

**MORE
POWERFUL
TOGETHER**

Subprocessors

This Appendix sets out the Subprocessors Oleeo uses to help provide the Services.

Oleeo engages the following Subprocessors and the Client agrees all of these Subprocessors may have access to Client Personal Data in line with the Services and functionality used, as listed in the Oleeo Subprocessor table.

<List of subprocessors used to be inserted>

End Of Data Processing Agreement



Service Level Agreement

This Service Level Agreement is incorporated and forms part of the Supplier Terms

This Service Level Agreement is incorporated and forms part of the Supplier Terms

Definitions

The following terms in capitals used in this Service Level Agreement shall have the following meanings:

“Client” means Buyer

“Client Data” means Buyer Data

“Client User” means Buyer User

“Oleeo” means Supplier

I HOSTING SERVICES

1. Service Availability

1.1 Terms capitalised in this Schedule shall have the following meaning:

“Availability” relates to the availability of the System to Candidates and Client Users. It is stated by showing unscheduled unavailability as a percentage of the measurement period i.e.:

Availability = Measurement period – Unscheduled unavailability x 100 % Measurement period

“System Response Time” means the number of seconds for a server to respond to a request from the time it receives a request

1.2 Availability is measured by Alertsité or other independent third Party Oleeo may select from time-to-time. The System is deemed unavailable when authentication to the service is not possible (via SSO or the login page)

1.3 The measurement period for this Service Level is monthly less planned maintenance time. Oleeo will provide monthly reports on the service availability to the Client on request.

1.4 Oleeo shall, ensure that the System, during any calendar month from the Go Live Date, is available to Client Users and Candidates for more than 99.9% of the total possible uptime during that month (excluding any scheduled downtime which is necessary to effect any essential modifications or maintenance to the Server).

1.5 Service Availability Target

Availability	99.9% over any calendar month
System Response Time	6 second average over any calendar month
Service Provision	24 hrs x 7 days excluding the Planned Maintenance Window

1.6 Oleeo undertakes planned Maintenance in the Planned Maintenance Window, and may undertake Ad Hoc Maintenance outside Maintenance Hours by giving notice, set out below (Oleeo will make reasonable endeavours to undertake any ad hoc maintenance outside of Business Hours):

Maintenance Activity	Window/ Notice Period
Planned Maintenance Window	22:00 – 02:00 GMT
Ad Hoc Maintenance Notice	Minimum of 8 Working Hours' notice (except in emergencies)

1.7 Planned downtime is not included in the calculation of unavailability under this document. Wherever possible, Oleeo will agree the outage with the Client in advance of the required work:

2. Backup Servers

2.1 Oleeo shall at all times for the duration of this Agreement ensure that it has access to a backup server.

2.2 If the hosting server ("**Server**") develops any problem or defect, Oleeo shall as soon as practicable in the circumstances transfer the System from the Server to a backup server (the "**Backup Server**"). If the Server's problem or defect has been corrected, Oleeo may transfer the System back to the Server.

2.3 Oleeo will store Client Data for a defined period as detailed in the DPA. Thereafter Client Data will be deleted.

2.4 Oleeo shall use its reasonable endeavours to ensure:

2.4.1 the Server is and will remain accessible to Client Users and Candidates via the Internet (subject only to reasonable and scheduled maintenance work at times which shall cause the least amount of interruption to Client Users and Candidates wishing to use the Web Site);

2.4.2 the Server remains in good working order and condition to enable Oleeo to comply with its obligations under this paragraph 2.4; and

2.4.3 any areas within the System which are restricted to individual Client Users or groups of Client Users will not be accessible to Client Users or Candidates generally unless the Client User requesting access thereto is entitled to obtain access thereto (whether through the use of a valid password or otherwise).

II MAINTENANCE SERVICES

1. Maintenance

1.1 Oleeo shall ensure that the System continues to function properly for the duration of this Agreement and shall continuously monitor the System operation during Business Hours to ensure the proper functioning thereof.

1.2 If the System becomes defective, Oleeo shall:

1.1.1 if notified by the Client during Business Hours, respond within 60 minutes of such notification;

1.1.2 if notified by the Client outside of Business Hours, respond by no later than 09:30 on the Business Day immediately following the day on which such notification was received; or

1.1.3 on becoming aware that the System does not function properly, immediately notify the Client.

1.3 Oleeo shall, if the System fails to function properly, commence remedial work as soon as may be practicable in the circumstances, and shall, during Business Hours, use its reasonable endeavours to remedy any defect in the System.

2. New Versions of the System



2.1 Oleeo shall from time to time make new versions of the System generally available to its customers. Such new versions shall be available to the Client at no cost.

3. Bug Fixes and Enhancements

3.1 Oleeo reserves the right to promote changes to the production environment as appropriate for the purposes of bug fixing, enhancements and providing new features. Where these changes may impact the Client Oleeo shall:

3.2 Use its reasonable endeavours to provide appropriate details of the changes prior to release (five (5) working days where impact is considered not negligible); and

3.3 Ensure that proper quality control and change control processes are followed internally to reduce the likelihood of any impact on the Client.

III SUPPORT SERVICES

1. Helpdesk & Support

1.1 Oleeo shall provide the following **"Help Desk"** to the Client to enable the Client to report problems with the functioning or operation of the System or to require assistance in respect of the System.

1.2 Oleeo offers Help Desk Services through a customer support portal (available 24/7) and Help Desk Staff (available during Business Hours only)

1.3 Oleeo shall make available a sufficient number of personnel who are sufficiently skilled in the operation of the System ("**Help Desk Staff**") to respond to support queries.

1.4 Oleeo shall ensure that any support queries received from the Client are responded to:
1.4.1 within 60 minutes from receipt of a request, if the request was made during Business Hours;
or
1.4.2 before 09:30am on the next Business Day if the request was received outside of Business Hours.

1.5 Oleeo shall ensure that the Help Desk Staff:
1.5.1 use reasonable endeavours to provide any required assistance in the use and/or operation of the System; and
1.5.2 escalate any such request to a suitably qualified personnel if the Help Desk Staff is unable to provide the required assistance.

1.6 Oleeo will work to the Service Levels within this Service Level Agreement providing the Client is not in breach of its obligations under the Agreement and does not exceed the stated number of maximum Candidates, FTE, Users and or Supported Users, where defined in the Order Form. Where maximum Candidate numbers are defined in the Order Form, Clients should therefore make the Oleeo Helpdesk aware of any significant increase in Candidate applications, especially those anticipated as a consequence of running one off campaigns or seasonal recruitment programmes.

1.7 Should Clients use of the Help Desk become excessive due to a lack of system training or knowledge, Oleeo reserve the right to either insist on further training or an increase in the monthly hosting fee.

2. Support Service Availability Target

Service Provision	During Business Hours
Service provision is defined as the following Services:	



Supported User Support: Support to Supported Users – All queries to be responded to within 60 minutes within the above service provision times.

Candidate Support (if purchased): Support for Candidates via a defined email address – All queries to be responded to within 48 hours within the above service provision times.

3. Fault & Service Request Handling

Oleeo will assess, classify and prioritise all incidents using the following guidelines:

Priority	Impact	Fault	Service Request
1	Critical: service affecting	Complete system crash – System is completely unavailable. There is a critical security incident.	Change required ensuring that the solution becomes and remains operable.
2	Severe: service affecting	Some day to day work can be completed but business is impacted. Multiple applications are unavailable. There is a high risk to the security of the Oleeo service.	Change required maintaining a main element of the solution.
3	Moderate: not service affecting	The service is available but day to day business may be moderately impacted. One or more business applications are unable to operate fully. There is a moderate risk to the security of the Oleeo service.	Change required improving element of the solution.
4	Low: not service affecting	The service is available and most or all daily tasks can still be carried out All applications can be used but some features are affected. There is a low risk to the security of the Oleeo service.	Cosmetic Change required to an element of the solution.

3.1 Incidents classified as a Priority 1 or 2 identified by Oleeo will be reported to the Client. During the lifecycle of each incident, until it is resolved and closed, Oleeo will provide regular status updates to the Client.

4. Acknowledgement and Resolution Start

Oleeo aims to acknowledge all support requests and attempt resolution within an hour. Should a resolution not be immediately achievable the following target service levels will apply depending on the priority of the fault:

Target times for fault acknowledgement and resolution start	
Priority	Response Times
1	If not recoverable immediately, start to develop a solution within 4 hours.
2	If not recoverable immediately, start to develop a solution within 8 hours.
3	If not recoverable immediately, start to develop a solution within 24 hours.
4	If not recoverable immediately, start to develop a solution within 72 hours.

5. Change Requests

A Change Request occurs when the Client asks for a configuration change, which is not due to a fault or maintenance problem. Target times, and associated costs, for servicing Change Requests are dependent on the nature of the request, will be agreed on a case-by-case basis.

6. Training



Oleeo will provide training as set out in the Order Form or Statement of Work. Additional training will be provided at the Daily Rates as per the Order Form or Statement of Work.

IV SECURITY REQUIREMENTS

1. Security Requirements

1.1 Users will be given unique individual access.

1.2 By default, Users will be subject to "three strikes and you're out", which means that they will be refused access to those parts of the System which require password access if they entered a wrong login name and password on three consecutive occasions until they contact Oleeo to obtain access again

1.3 The Client will take appropriate measures against and be responsible for any misuse of the System or data by the Users.

2. Database Security

2.1 Oleeo shall keep and maintain a back-up copy of the Database and shall, if the Database (or any part thereof) is in any way damaged, destroyed, modified in an unauthorised way or becomes corrupted:

2.1.1 use a back-up copy to replace the damaged, destroyed, modified or corrupted copy of the Database;

2.1.2 notify the Client in writing of such damage, destruction, modification or corruption and the reasons therefore (if known to Oleeo); and

2.1.3 take whatever steps may be practicable in the circumstances to avoid any such damage, destruction, modification or corruption from occurring again.

2.2 Oleeo shall back-up the Database onto a hard-drive at the end of each Business Day.

3. Data Retention

In the absence of other instruction, Oleeo will assume the Clients data retention policy is to retain Candidate data for 12 months; Oleeo will periodically review the Client system and inform the Client if there is data that exceeds the applicable retention period.

4. Penetration testing

Oleeo will engage an accredited third party on an annual basis to conduct a penetration test of the System. If the Client wishes at any point to conduct its own security review, it may do so under terms and conditions prescribed by Oleeo, at its sole discretion and subject to Oleeo's then applicable charges, which are available on request.

5. Audit and security

Oleeo provide access to standard "Non-protectively Marked" Oleeo audit and security policy documents free of charge but reserves the right to charge at the applicable rates set out in Schedule 1 for any requests for additional information not contained within such documents and/or additional resources required by the Client from Oleeo to assist with an audit or other security requirements. Oleeo will maintain accreditation to ISO 27001:2022 or a later equivalent for the duration of the term. Oleeo may modify or update the Security Requirements at its sole discretion provided that such modification or update does not result in a material degradation in the security protection offered by Oleeo.

