DeepQ AI Platform Terms of Use

Update on: Febrary 20, 2024

Thank you for using the DeepQ AI Platform (the "**Platform**"). Please read these DeepQ AI Platform user terms and conditions (the "**Terms**") and any additional terms, exhibits provided to You by DeepQ when using the Platform ("**Additional Terms**", the "**Terms**" and "**Additional Terms**" are collectively referred to as the "**User Terms**") carefully to understand your rights and responsibilities. By using the Platform or any product or service available within, you agree to be bound by the User Terms. If You do not agree to any provision of the User Terms, please do not use the Platform.

You understand that the User Terms may be amended from time to time. Amended User Terms will be published when the Platform software is updated or upgraded or posted on the website run by DeepQ. Your continued access to or use of the Platform following the publishing or posting of the amended User Terms means that You accept and agree to any amended User Terms. You are expected to check this page each time You access or use the Platform to keep Yourself informed of any changes that are binding on You. If there is a conflict or inconsistency between the Terms and the Additional Terms, the Additional Terms shall prevail.

1. **DeepQ AI Platform.** The Platform is a machine learning model platform developed and operated by DeepQ Technology Corporation ("**DeepQ**"), which provides the users with a machine learning model training environment. The users can upload their dataset to the Platform through the web page management interface to engage in machine learning model training and data annotation (the "**Services**"). The data that You upload are collectively referred to as "**User Data**".

2. **Age Minimum.** The Services are provided to users who are at least sixteen (16) years old (and at least the legal age in Your jurisdiction). You promise that You are at least sixteen (16) years old (and at least the legal age in Your jurisdiction) when using or accessing to the Platform. If You are under the age of sixteen (16) or under the age of majority or age subject to parental consent according to applicable laws in Your jurisdiction, You should obtain the approval of Your parents or the person(s) with parental responsibility and review the User Terms together with them to ensure that You and Your parents or the person(s) with parental responsibility understand and agree to the User Terms.

3. **Establishing an Account.** To use certain functions of the Platform, You are required to register an account with the Platform. If You are authorized to register an account on behalf of Your employer or organization, You will be bound by the User Terms and the user account policy published by Your employer or organization. You should keep Your login credentials away from any third party, and do not authorize it to use Your login credential or share Your login credentials with it. If You register an account with the Platform by Yourself or on behalf of Your employer or organization, You or Your employer or organization accept responsibilities for all activities that occur under Your or Your employer or organization's account. If You notice someone else is using Your account without Your permission, notify the system administrator of Your employer or organization without delay. If You are the administrator account owner, you have the right to set up the account for the group member; when You set up the account for the

group member, You guarantee that You have obtained the group member's consent to legally use the his/her email and other information to set up the account.

4. **System Requirements.** To use the Services provided through the Platform, You will need a computer that is connected to internet, internet connection and other compatible software. You understand that these system requirements may change from time to time and affect Your ability to access and use Services on the Platform. You shall be solely liable for these system requirements and the associated costs (for example the costs of internet).

5. **Platform Services.**
    a. The Platform is a management and service platform for machine learning model training. You can upload User Data for machine learning model training and data annotation through the Platform. You can manage the User Data that You have uploaded through the management page of the Platform. If You have any questions while using the Platform, You may contact DeepQ and DeepQ will provide You with necessary assistance, including but not limited to User Data upload testing, changing the User Data file format and deleting User Data.
    b. The Platform may provide the functionality that the project owner who uploads the dataset can invite third party to participate in individual project (including other machines learning training tools available on the Platform). If You invite third parties to participate in Your project, You should determine and manage the role and corresponding authority for such third parties. You shall be solely responsible for such third parties' management and exercise of authority. You should have the invited third parties appropriately exercise the authority granted by You.
    c. The Platform only provides a machine learning model training environment. DeepQ does not warrant the correctness, legality or completeness of the User Data that you upload. You shall ensure that the User Data that You upload, as well as the processing and use of the User Data, is in compliance with applicable laws, including but not limited to personal information protection related laws. In addition, You will be solely responsible for the correctness, legality or completeness of the User Data that you upload.
    d. **You SHALL NOT upload any data with personal information to the Platform or provide DeepQ with such data**, otherwise you are subject to the obligations under Article 18 (Indemnification). If the data You upload might include personal information, You warrant that You or Your employer or organization have/has obtained the written consent from the data subjects and been in compliance with all applicable laws, policies, and regulations, especially those relating to the collection of information from data subjects. If You upload the data in DICOM format and the Platform detects any personally identifiable information (such as names and ID of the data subjects, in the form of metadata), the Platform may, at our sole discretion, remove such detected metadata before processing. However, DeepQ does not guarantee all personally identifiable information in DICOM tags can be completely removed.
    e. In cases where You upload any data with personal information to the Platform or share it with DeepQ, the Data Processing Addendum set forth in Exhibit I, the Standard Contractual Clauses set forth in **Exhibit II** and Business Associate Agreement set forth in **Exhibit III**, in addition to the main body of the User Terms, shall govern the relationship between You and DeepQ. Please refer to the applicable exhibit(s) for specific terms.

Exhibit I, Exhibit II and **Exhibit III** apply as follows: (i) if the relationship between You and DeepQ is subject to GDPR and involves a cross-border transfer, the terms in **Exhibit I** and **Exhibit II** will prevail; (ii) if the relationship between You and DeepQ is subject to GDPR but not involves a cross-border transfer, the terms in **Exhibit I** will prevail; (iii) if the relationship between You and DeepQ is subject to HIPAA, the terms in **Exhibit III** will prevail; (iv) if the relationship between You and DeepQ is neither governed by GDPR nor HIPAA, the terms in **Exhibit I** will prevail. If the relationship between You and DeepQ is governed by applicable privacy and security laws other than GDPR and HIPAA, the requirements of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 referred in **Exhibit I** and the requirements of 45 CFR 160.103 referred in **Exhibit II** will be replaced with that of the applicable laws to the extent appropriate and permitted by such applicable laws.

f. You warrant that all data You upload is lawfully obtained and used. It is Your sole responsibility if the way You obtain and use the data You upload is in violation of applicable laws.
g. Unless otherwise provided in the User Terms, the Privacy Policy of this Platform, or agreed by Your employer or organization who entered into the license agreement with DeepQ, DeepQ will not view, collect, process or share with any third party all data that you upload, provide, or key in, including the User Data. However, if (i) required by applicable laws or governmental authorities, or (ii) for the purpose of protecting the information security of the Platform, or improving the Platform performance or quality of Services provided by the Platform, or addressing Your needs for technical support, DeepQ may access or view the data annotation and User Data that You upload.
h. The service products resulting from Your use of the Services, including but not limited to the trained machine learning models ("**Service Products**"), can only be used by You on the Platform during the term of the Service or trial Service in a manner that is in compliance with the User Terms.

6. **Data Backup.** The Platform does not provide data backup and hosting Services, (i) DeepQ does not guarantee that the User Data You upload will not be removed, damaged, destroyed, lost or become no longer available; (ii) You should make Your own regular backups of the User Data that You upload to the Platform, as well as information that You acquire from the use of the Services on the Platform. Upon termination of the User Terms, the Services or trial Services, DeepQ will follow internal procedure to destroy the User Data that You uploaded. If You wish to keep the User Data that You upload, You should give DeepQ a written notice before the termination of the User Terms, the Services or trial Services. DeepQ will contact You for the data storage agreement as soon as practicable.

7. **DeepQ Licenses.** Subject to Your full compliance with the User Terms, DeepQ grants You a limited, personal, non-assignable, non-exclusive and revocable license to access and use the Platform controlled and operated by DeepQ, the Services and the Service Products, **for personal and non-commercial purposes** during Your applicable trial, rental, purchase or license period, or the period during which DeepQ is entitled to provide You with the Services. **The Platform, the Services and the Service Products cannot be used for clinical trial, for medical or commercial purposes, or in any matter other than those permitted in the User Terms**.

8. **License Restrictions.** If You breach this User Terms, DeepQ may immediately terminate Your right to use of the Platform, the Services, the Service products, products and/or DeepQ related accounts, without any refunds. The license under Article 7 is subject to Your compliance with the below requirements. You shall not:
    a. Work around any technical restriction in the Platform, or to use the Platform in an attempt to, or in conjunction with any device, program or service to circumvent the technical restrictions to control access to the Platform;
    b. Attempt to access the source code related to the Platform through reverse engineering, decoding, de-compilation, reverse compilation or otherwise, except and only to the extent that applicable law expressly permits, despite this limitation;
    c. Sell, lease, rent, re-distribute, broadcast, revise, sublicense, assign or otherwise transfer to any third party any software, algorithm on the Platform or Your right to use the Platform without authorization, unless otherwise provided in the applicable end user license agreement between You, Your employer or organization and DeepQ;
    d. Modify or make any derivative works of the Platform, any Service or Service Products in whole or in part;
    e. Remove any proprietary notices or labels on the Platform, any Service, the Service Products or their copy;
    f. Use the Platform, any Service or Service Products for clinical trial, medical or commercial purposes, or in any manner other than those permitted in the User Terms, unless otherwise provided in the applicable end user license agreement between You, Your employer or organization and DeepQ;
    g. Display (in part or in whole) the Platform, any Service or Service Products as part of any public performance or display even if no fee is charged, unless otherwise provided in the applicable end user license agreement between You, Your employer or organization and DeepQ;
    h. Use the Platform, any Service provided on the Platform or Service Products to infringe upon the rights of DeepQ, its affiliates or any third party, or use the Platform, any product, the Services or the Service Products in any way that does not comply with all applicable law or any applicable end user license agreement between You, Your employer or organization and DeepQ;
    i. Use any automated tool on the Platform to engage in any activity that is not related to machine learning training, such as exploring the vulnerability of external websites, malicious attack on other websites, attempt to alter, damage or scan the Services in an undue manner or interfering other users; or
    j. Use the Platform, the Service provided on the Platform or Service Products in any manner not specifically permitted by the User Terms.

9. **Support and Update.** Unless otherwise provided in the User Terms, DeepQ has no obligation and may not provide any support services to the Platform, any Service published through the Platform, or Service Products.

10. **Privacy.** To use the Platform or certain function of the Services available through the Platform, You may be required to provide certain personal information, including Your name, email address and passwords to create the account. DeepQ will collect, process and store the personal information provided during Your use of the Platform and protect Your privacy in accordance with the Privacy Policy of the Platform. Please read the Privacy Policy carefully.

11. Acceptable Use Policy

a. You agree that when accessing and using the Platform You will not engage in or attempt to engage in any improper use, including but not limited to any use that violates DeepQ Code of Conduct.

b. If DeepQ suspects violations of these Terms, DeepQ may institute legal action, and cooperate with legal enforcement authorities in bring legal proceedings against the violators. Unless otherwise prohibited by applicable laws, You agree to cooperate with DeepQ in the investigation into any suspicious violation by You or any other person. You hereby authorize DeepQ to install, implement, manage and operate one or multiple types of software or monitoring measures or take other measures to ascertain the activities in violation of applicable laws or the User Terms, or to track any activities deemed possibly in violation of applicable laws or the User Terms by DeepQ.

12. **Ownership of Intellectual Property Rights.**

a. Unless otherwise provided in the User Terms or the applicable end user license agreement between You or Your employer or organization and DeepQ, DeepQ and its affiliates, authorized third parties and suppliers own the title, intellectual property rights and other proprietary rights of the Platform, the Services provided on and through the Platform and the Service Products (and all rights embodied therein) and reserve any right that has not been expressly granted to You under the User Terms. The DeepQ related logo and other names of DeepQ products and Services on the Platform are the trademarks and logos of DeepQ and its affiliates. In addition, any other third party company name, product name, service name or logo related to any product or services published on or through the Platform may be trademark or logo owned by other third parties and shall not be used without their permission.

b. The Platform may include third party software governed by open source or third party license terms ("**Third Party Terms**"). Your use of such third party software shall be subject to the restrictions set forth by any Third Party Terms. You can further understand the third party software and the Third Party Terms applicable to them on the settings page of the Platform.

13. **Feedback.** In addition to the User Data that You upload in accordance with the User Terms, You may provide verbal or written comments, suggestions, ideas, plans, explanations, drawings or other information related to the Platform or Services ("**Feedback**"). DeepQ is free to use, disclose, reproduce, license or otherwise distribute such Feedback without any obligations to You.

14. **Termination.** If You breach any provision of the User Terms, the User Terms shall terminate automatically. You may terminate the User Terms at any time by cancellation of Your account. You understand that the termination of the User Terms will not entitle You to any refund, including any fee related to any subscription plan. Upon termination of the User Terms, the Services or the trial Services, or expiration of the Services or the trial Services, You must immediately stop using the Platform and the below clauses of the User Terms shall survive the termination or expiration: first part of Articles 5 (d), Articles 5 (e) (as the case may be), Articles 5 (f), the last paragraph of Article 7, Articles 8 to 26. DeepQ reserves the right to change, remove, delete, restrict or prohibit use or cease all or part of the rights and licenses granted to You related to the Platform, any Services or Service Products at any time without prior notice to You.

15. **DISCLAIMER.** TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE PLATFORM,ALL SERVICES PROVIDED THROUGH THE PLATFORM AND SERVICE PRODUCTS ARE PROVIDED TO YOU "AS IS", "WITH ALL FAULTS" AND "AS AVALIABLE" AND THE ENTRIE RISK OF USE AND PERFROAMNCE, REMAINS WITH YOU. DEEPQ AND ITS SUPPLIERS AND LICENSORS DO NOT MAKE ANY REPRESENTATIONS, WARRANTIES, OR CONDITIONS, EXPRESS, IMPLIED, OR STATUTORY, AND HEREBY DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY, MERCHANTABLE QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, QUIET ENJOYMENT, OR NONINFRINGEMENT. IN PARTICULAR, DEEPQ, ITS SUPPLIERS AND LICENSORS MAKE NO WARRANTY THAT THE PLATFORM, ANY SERVICES AVAILABLE WITHIN OR SERVICE PRODUCTS: (I) WILL MEET YOUR REQUIREMENTS OR WILL WORK WITH ANY THIRD-PARTY SOFTWARE, APPLICATIONS OR THIRD-PARTY HARDWARE; (II) WILL BE AVAILABLE OR PROVIDED ON AN UNINTERRUPTED, TIMELY, SECURE OR ERROR-FREE BASIS; (III) OR ANY INFORMATION OR CONTENT OBTAINED THROUGH IT WILL BE ACCURATE, COMPLETE, OR RELIABLE; OR (IV) THAT ANY DEFECTS OR ERRORS THEREIN WILL BE CORRECTED. ALL SERVICES AVALIABLE FOR YOU AND OTHER MATERIAL YOU DOWNLOAD OR ACCESS AND USE THROUGH THE PLATFORM ARE AT YOUR OWN RISK, AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE OR LOSS THAT RESULTS THEREFROM. USE OF THIS PLATFORM MAY AFFECT THIRD-PARTY HARDWARE, SOFTWARE, APPLICATIONS, DEVICES, OR SERVICES. YOU MAY HAVE ADDITIONAL RIGHTS UNDER YOUR LOCAL LAWS THAT THESE TERMS CANNOT CHANGE. IN PARTICULAR, TO THE EXTENT LOCAL LEGISLATION IMPLIES STATUTORY TERMS WHICH CANNOT BE EXCLUDED, THOSE TERMS ARE DEEMED INCORPORATED INTO THESE TERMS BUT DEEPQ'S LIABILITY FOR A BREACH OF THOSE STATUTORY IMPLIED TERMS IS LIMITED IN ACCORDANCE WITH AND TO THE EXTENT PERMISSIBLE UNDER THAT LEGISLATION.

16. **DISCLAIMER AGAINST SPECIFIC DAMAGES.** IN NO EVENT WILL DEEPQ OR ANY SUPPLIER OR LICENSOR BE LIABLE FOR ANY CONSEQUENTIAL; SPECIAL; INCIDENTAL; DIRECT; INDIRECT; PUNITIVE DAMAGES; FOR LOSS OF PROFITS, BUSINESS, GOODWILL, ANTICIPATED SAVINGS, OR USE; LOSS OR CORRUPTION OF DATA, CONFIDENTIAL INFORMATION, OR OTHER INFORMATION; BUSINESS INTERRUPTION; PERSONAL INJURY; PROPERTY DAMAGE; LOSS OF PRIVACY;

FAILURE TO MEET ANY DUTY OF GOOD FAITH OR REASONABLE CARE; NEGLIGENCE; AND ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER, ARISING OUT OF, BASED ON, RESULTING FROM OR IN ANY WAY RELATED TO THESE TERMS, THE PLATFORM, ANY SERVICE(S) AND/OR THE SERVICE PRODUCTS, EVEN IF DEEPQ OR ANY SUPPLIER OR LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGE, LOSS, OR LIABILITY FROM INTENTIONAL ACTS (INCLUDING FRAUD, FRAUDULENT MISREPRESENTATION, AND FAILURE TO DISCLOSE DEFECTS), PRODUCT LIABILITY, OR FOR DEATH OR PERSONAL INJURY. NOTHING IN THIS SECTION 16 WILL BE INTERPRETED AS EXCLUDING LIABILITY WHICH CANNOT UNDER APPLICABLE LAW BE EXCLUDED IN THOSE JURISDICTIONS. IF YOU LIVE, OR ARE OTHERWISE SUBJECT TO THE LAWS IN ONE OF THOSE JURISDICTIONS, ANY STATUTORY ENTITLEMENT AVAILABLE TO YOU WILL BE DEEMED LIMITED TO THE EXTENT (IF AT ALL) PERMISSIBLE UNDER THAT LAW AND, IF LIMITATION IS NOT PERMITTED, THE LIMITATIONS AND EXCLUSIONS IN THIS SECTION 16 MAY NOT APPLY TO YOU.

17. **LIMITED LIABILITY AND SOLE REMEDY.** TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND TO THE EXTENT THEY ARE NOT EXCLUDED OR DISCLAIMED UNDER SECTION 16, DEEPQ'S AND ITS SUPPLIERS' AND LICENSORS' MAXIMUM, AGGREGATE LIABILITY TO YOU, AND YOUR EXCLUSIVE REMEDY UNDER THE USER TERMS FOR ANY AND ALL DAMAGES, INJURIES, AND LOSSES ARISING FROM ANY AND ALL CLAIMS AND CAUSES OF ACTION ARISING OUT OF, BASED ON, RESULTING FROM OR IN ANY WAY RELATED TO THE USER TERMS, THE PLATFORM, ANY SERVICES AVAILABLE WITHIN AND THE SERVICE PRODUCTS WILL BE TO RECOVER OF: THE ACTUAL DAMAGES YOU INCUR BASED UPON REASONABLE RELIANCE ON THE PLATFORM, ANY SERVICES AVAILABLE WITHIN UP TO FIVE DOLLARS (US $5.00).

    THE EXISTENCE OF MULTIPLE CLAIMS OR SUITS UNDER OR RELATED TO THE USER TERMS, THE PLATFORM, THE SERVICES, THE SERVICE PRODUCTS, OR THE PROVISION OR FAILURE TO PROVIDE SUPPORT WILL NOT ENLARGE OR EXTEND THE LIMITATION OF MONEY DAMAGES. EXCEPT FOR THE EXCLUSIVE REMEDY IN THE FOLLOWING SENTENCE, THESE ACTUAL MONEY DAMAGES WILL BE YOUR SOLE AND EXCLUSIVE REMEDY.

    SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGE, LOSS, OR LIABILITY FROM INTENTIONAL ACTS (INCLUDING FRAUD, FRAUDULENT MISREPRESENTATION, AND FAILURE TO DISCLOSE DEFECTS), PRODUCT LIABILITY, OR FOR DEATH OR PERSONAL INJURY. NOTHING IN THIS SECTION 17 WILL BE INTERPRETED AS EXCLUDING LIABILITY WHICH CANNOT UNDER APPLICABLE LAW BE EXCLUDED IN THOSE JURISDICTIONS. IF YOU LIVE, OR ARE OTHERWISE SUBJECT TO THE LAWS IN ONE OF THOSE JURISDICTIONS, ANY STATUTORY ENTITLEMENT

AVAILABLE TO YOU WILL BE DEEMED LIMITED TO THE EXTENT (IF AT ALL) PERMISSIBLE UNDER THAT LAW AND, IF LIMITATION IS NOT PERMITTED, THE LIMITATIONS AND EXCLUSIONS IN THIS SECTION 18 MAY NOT APPLY TO YOU.

EXCEPT FOR DISPUTES IN WHICH EITHER PARTY SEEKS TO BRING AN INDIVIDUAL ACTION IN SMALL CLAIMS COURT, YOU AND DEEPQ AGREE THAT ANY DISPUTE MUST BE COMMENCED OR FILED BY YOU OR DEEPQ WITHIN ONE (1) YEAR OF THE DATE THE DISPUTE AROSE, OTHERWISE THE UNDERLYING CLAIM IS PERMANENTLY BARRED (WHICH MEANS THAT YOU AND DEEPQ WILL NO LONGER HAVE THE RIGHT TO ASSERT SUCH CLAIM REGARDING THE DISPUTE)..

18. **INDEMNIFICATION.** You will defend, indemnify, and hold harmless DeepQ, its directors, officers, employees, agents, partners, suppliers, and licensors and will keep them indemnified from any third party claim or demand, including reasonable attorneys' fees, relating to or arising from (i) Your unauthorized use of the Platform, any Services and/or Service Products; (ii) any violation by You of the User Terms; (iii) Your violation of any another party's rights or applicable law; or (iv) any User Data You provide.

19. **Restricted Use.** The Platform, the Services provided through the Platform and Service Products are not designed for system that do not require fail-safe performance. You may not use the Platform, Services through the Platform or Service Products in any device or system in which a malfunction would result in foreseeable risk of injury or death to any person. This includes operation of nuclear facilities, aircraft navigation or communication systems and air traffic control.

20. **Dispute Resolution, Governing Law and Jurisdiction.** Except as otherwise provided herein, the interpretation of the User Terms or any dispute or disagreement arising out of any breach of this User Terms shall be governed by the laws of Taiwan, regardless of conflict of laws principles. All other claims, including any claim arising out of the Consumer Protection Act, Unfair Competition Act or any act of torts, shall be governed by the laws of the country or territory where You reside. Except as otherwise provided herein, You irrevocably agree that any dispute arising out of the User Terms or any matter related hereto shall be resolved by the Taiwan Taipei District Court. If the applicable law does not allow for the designation of the Taipei District Court as the first-instance court, the court of jurisdiction shall be determined in accordance with the applicable laws.

21. **Legal Effect.** The User Terms do not change Your rights under the laws of the country in which You reside if the laws of Your country do not permit it to legally change Your rights. You may have rights under the laws of the country in which You reside that are in addition to, or different from, the rights set forth in the User Terms.

22. **Compliance with Law and Export Regulations:** You will comply with all national or international laws, regulations and legislations applicable to this Platform, any Service available through the Platform and/or Service Products, including but not limited to the US Export Administration Regulations (software is subject to these regulations), as well as any relevant restrictions on users, purpose of use and destination promulgated by the governments.

23. **General Terms.** The titles of the clauses of the User Terms are provided for the parties' convenience only and shall not carry any legal or contractual meaning. If DeepQ does not take any action against Your breach, it does not constitute a waiver of its right to take action against any subsequent or similar breach. No waiver of any clause of the User Terms shall be valid unless it is signed in writing. No waiver shall be deemed a waiver of a similar clause or any other clause. If a court of competent jurisdiction rules that any terms, covenant or restriction of the User Terms is illegal, invalid or unenforceable, the remaining terms or restrictions shall remain in full force and effect, and will in no way be affected, impaired or invalidated. You may not assign, transfer or sublicense any of Your rights (if any) under the User Terms. The User Terms are binding on all DeepQ successors and assignees.

24. **Entire Agreement.** Unless otherwise provided in the applicable end user license agreement between You, Your employer or organization and DeepQ, the User Terms constitute the entire agreement for the license and use of the Platform, any Services and Service Products.

25. **Contact Information.** If you have any question about the User Terms, please send all notices and letters to:

    To: DeepQ Technology Corporation

    Attention: Data Protection Officer

    13F., No. 207-5, Sec. 3, Beixin Rd.

    Xindian District, New Taipei City 231 Taiwan

Exhibit I

Data Processing Addendum

Your use of certain services and products from DeepQ Corporation (including its affiliates, "**DEEPQ**") may involve processing personal information. To the extent that the applicable agreement, ("**Agreement**") state that DEEPQ process personal information as Your processor, these Data Processing Addendum (including its appendices, the "**Addendum**") apply.

1 **Overview**

This Addendum describes the parties' obligations, including under applicable privacy, data security, and data protection laws, with respect to the processing and security of Customer Data (as defined below). This Addendum will be effective on the Addendum Effective Date (as defined below), and will replace any terms previously applicable to the processing and security of Customer Data. Capitalized terms used but not defined in this Addendum have the meaning given to them in the Agreement.

2 Definitions

2.1 In this Addendum:

2.1.1 "Addendum Effective Date" means the earlier date on which You accepted, DEEPQ provides the applicable Services, or the parties otherwise agreed to, this Addendum.

2.1.2 "Applicable Privacy Law" means, as applicable to the processing of Customer Personal Data, any national, federal, European Union, state, provincial or other privacy, data security, or data protection law or regulation.

2.1.3 "Customer Data" has the same meaning in the Agreement.

2.1.4 "Customer Personal Data" means the personal data contained within the Customer Data, including any special categories of personal data or sensitive data defined under Applicable Privacy Law.

2.1.5 "Data Incident" means a breach of DEEPQ's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by DEEPQ.

2.1.6 "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, and repealing Directive 95/46/EC.

2.1.7 "European Data Protection Law" means, as applicable: (a) the GDPR; or (b) the Swiss FADP.

2.1.8 "European Law" means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data); or (c) the law of Switzerland (if the Swiss FADP applies to the processing of Customer Personal Data).

2.1.9 "GDPR" means, as applicable: (a) the EU GDPR; or (b) the UK GDPR.

2.1.10 "DEEPQ's Third-Party Auditor" means a DEEPQ -appointed, qualified and independent third-party auditor, whose then-current identity DEEPQ will disclose to You.

2.1.11 "Instructions" has the meaning given in Section 5.2 (Compliance with Your Instructions).

2.1.12 "Notification Email Address" means the email address(es) designated by You in the Agreement or writing from You to receive certain notifications from DEEPQ.

2.1.13 "Security Measures" has the meaning given in Section 6.1.1 (DEEPQ's Security Measures).

2.1.14 "Services" has the same meaning in the Agreement.

2.1.15 "Subprocessor" means a third party authorized as another processor under this Addendum to process Customer Data in order to provide parts of the Services.

2.1.16 "Supervisory Authority" means, as applicable: (a) a "supervisory authority" as defined in

the EU GDPR; or (b) the "Commissioner" as defined in the UK GDPR or the Swiss FADP.

2.1.17 "Swiss FADP" means, as applicable, the Federal Act on Data Protection of 19 June 1992 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 14 June 1993) or the revised Federal Act on Data Protection of 25 September 2020 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 31 August 2022).

2.1.18 "Term" means the period from the Addendum Effective Date until the end of DEEPQ's provision of the Services, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which DEEPQ may continue providing the Services for transitional purposes.

2.2 The terms "personal data", "data subject", "processing", "controller", and "processor" as used in this Addendum have the meanings given by Applicable Privacy Law or, absent any such meaning or law, by the EU GDPR.

2.3 The terms "data subject", "controller" and "processor" include "consumer", "business", and "service provider", respectively, as required by Applicable Privacy Law.

3 Duration

Regardless of whether the applicable Agreement has terminated or expired, this Addendum will remain in effect until, and automatically expire when, the duration specified in this Addendum ends.

4 Roles; Legal Compliance

4.1 Roles of Parties. DEEPQ is a processor and You are a controller, or DEEPQ is a sub-processor and You are a processor, as applicable, of Customer Personal Data.

4.2 Compliance with Law. Each party will comply with its obligations related to the processing of Customer Personal Data under Applicable Privacy Law.

5 Data Processing

5.1 If You are a processor:

5.1.1 You warrant on an ongoing basis that the relevant controller has authorized:

5.1.1.1 the Instructions;

5.1.1.2 Your engagement of DEEPQ as another processor; and.

5.1.1.3 DEEPQ's engagement of Subprocessors as described in Section 10 (Subprocessors);

5.1.2 You will forward to the relevant controller promptly and without undue delay any notice provided by DEEPQ under Section 6.2.1 (Incident Notification), 8.2.1 (Responsibility for Requests), or 10.4 (Opportunity to Object to Subprocessors); and

5.1.3 You may make available to the relevant controller any other information made available by DEEPQ under this Addendum about the locations of DEEPQ data centers or the names, locations and activities of Subprocessors.

5.2 Compliance with Your Instructions. You instruct DEEPQ to process Customer Data in accordance with the Agreement (including this Addendum) and applicable law only as follows:

5.2.1 to provide, secure, and monitor the Services; and

5.2.2 as further specified via:

5.2.2.1 Your use of the Services; and

5.2.2.2 any other written instructions given by You and acknowledged by DEEPQ as constituting instructions under this Addendum (collectively, the "Instructions").

5.3 DEEPQ will comply with the Instructions unless prohibited by European Law, where European Data Protection Law applies, or prohibited by applicable law, where any other Applicable Privacy Law applies.

5.4 DEEPQ will process the personal data only for the specific purpose(s) of the processing, as set out in this Addendum, unless it receives further instructions from the controller.

6 Data Security

6.1 DEEPQ's Security Measures, Controls and Assistance.

6.1.1 DEEPQ's Security Measures. DEEPQ will implement and maintain technical, organizational, and physical measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in

Appendix 1 (Security Measures) (the "Security Measures"). The Security Measures include measures help ensure ongoing confidentiality, integrity, availability. DEEPQ may update the Security Measures from time to time provided that such updates do not result in a material reduction of the security of the Services. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects. If the processing involves sensitive data defined under Applicable Privacy Law, DEEPQ will apply specific restrictions and/or additional safeguards.

6.1.2 Access and Compliance. DEEPQ will:

6.1.2.1 authorize its employees, contractors and Subprocessors to access Customer Data only as strictly necessary to comply with Instructions; and

6.1.2.2 ensure that all persons authorized to process Customer Data are under an obligation of confidentiality.

6.1.3 DEEPQ's Security Assistance. DEEPQ will (taking into account the nature of the processing of Customer Personal Data and the information available to DEEPQ) assist You in ensuring compliance with its (or, where You are a processor, the relevant controller's) obligations relating to security and personal data breaches under Applicable Privacy Law, by:

6.1.3.1 implementing and maintaining the Security Measures in accordance with Section 6.1.1 (DEEPQ's Security Measures);

6.1.3.2 complying with the terms of Section 6.2 (Data Incidents);

6.1.3.3 providing the information contained in the applicable Agreement (including this Addendum); and

6.1.3.4 if subsections above are insufficient for You (or the relevant controller) to comply with such obligations, upon Your request, providing You with additional reasonable cooperation and assistance.

6.2 Data Incidents.

6.2.1 Incident Notification. DEEPQ will notify You promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.

6.2.2 Details of Data Incident. DEEPQ's notification of a Data Incident will describe: the nature of the Data Incident including Your resources impacted; the measures DEEPQ has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, DEEPQ recommends that You take to address the Data Incident; and details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, DEEPQ's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

6.2.3 No Assessment of Customer Data by DEEPQ. DEEPQ has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

6.2.4 No Acknowledgement of Fault by DEEPQ. DEEPQ's notification of or response to a Data Incident under this Section 6.2 (Data Incidents) will not be construed as an acknowledgement by DEEPQ of any fault or liability with respect to the Data Incident.

6.3 Your Security Responsibilities and Assessment.

6.3.1 Your Security Responsibilities. Without prejudice to DEEPQ's obligations under Sections 6.1 (DEEPQ's Security Measures, Controls and Assistance) and 6.2 (Data Incidents), and elsewhere in the applicable Agreement, You are responsible for Your use of the Services and storage of any copies of Customer Data outside DEEPQ's or DEEPQ's Subprocessors' systems, including:

6.3.1.1 using the Services to ensure a level of security appropriate to the risk to the Customer Data;

6.3.1.2 securing the account authentication credentials, systems and devices You use to access the Services; and

6.3.1.3 backing up or retaining copies of its Customer Data as appropriate.

6.3.2 Your Security Assessment. You agree that the Services, Security Measures, and DEEPQ's commitments under this Section 6 (Data Security) provide a level of security appropriate to the risk to Customer Data (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Data as well as the risks to individuals).

6.4 Reviews and Audits of Compliance.

6.4.1 Your Audit Rights.

6.4.1.1 Audit. DEEPQ will, if required under Applicable Privacy Law, allow You or an independent auditor appointed by You to conduct audits (including inspections) to verify DEEPQ's compliance with its obligations under this Addendum in accordance with Section 6.4.2 (Additional Business Terms for Reviews and Audits). During an audit, DEEPQ will reasonably cooperate with You or Your auditor as described in this Section 6.4 (Reviews and Audits of Compliance).

6.4.2 Additional Business Terms for Reviews and Audits.

6.4.2.1 You must contact DEEPQ's Team to request: an audit under Section 6.4.1.1.

6.4.2.2 DEEPQ and You will discuss and agree in advance on: the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 6.4.1.1.

6.4.2.3 DEEPQ may charge a fee (based on DEEPQ's reasonable costs) for any audit under Section 6.4.1.1. DEEPQ will provide You with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. You will be responsible for any fees charged by any auditor appointed by You execute any such audit.

7 DEEPQ will make available to You all information that is reasonably necessary to demonstrate DEEPQ's compliance with its obligations as a processor under the Addendum.

8 Access; Data Subject Rights; Data Export

8.1 Access; Rectification; Restricted Processing; Portability. During the Term, DEEPQ will enable You, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, and to export Customer Data. If You become aware that any Customer Personal Data is inaccurate or outdated, You will be responsible for using such functionality to rectify or delete that data if required by Applicable Privacy Law.

8.2 Data Subject Requests.

8.2.1 Responsibility for Requests. During the Term, if DEEPQ receives a request from a data subject that relates to Customer Personal Data and identifies You, DEEPQ will:

8.2.1.1 advise the data subject to submit their request to You;

8.2.1.2 notify You without undue delay; and

8.2.1.3 not otherwise respond to that data subject's request without authorization from You.

8.2.1.4 You will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

8.2.2 DEEPQ's Data Subject Request Assistance. DEEPQ will (taking into account the nature of the processing of Customer Personal Data) assist You in fulfilling its (or, where You are a processor, the relevant controller's) obligations under Applicable Privacy Law to respond to requests for exercising the data subject's rights by:

8.2.2.1 complying with Sections 8.1 (Access; Rectification; Restricted Processing; Portability) and 8.2.1 (Responsibility for Requests); and

8.2.2.2 if subsections above are insufficient for You (or the relevant controller) to comply with such obligations, upon Your request, providing You with additional reasonable cooperation and assistance.

9 Data Processing Locations and International transfers

9.1 Any transfer of data to a third country or an international organisation by DEEPQ shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

9.2 You agree that where DEEPQ engages a sub-processor in accordance with Addendum for carrying out specific processing activities (on behalf of the You) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

10 Subprocessors

10.1 Consent to Subprocessor Engagement. You specifically authorize DEEPQ's engagement as Subprocessors of DEEPQ's affiliates as of the Addendum Effective Date. In addition, without prejudice to Section 10.3 (Opportunity to Object to Subprocessors), You generally authorize DEEPQ's engagement of other third parties as Subprocessors ("**New Subprocessors**").

10.2 Requirements for Subprocessor Engagement. When engaging any Subprocessor, DEEPQ will:

10.2.1 ensure that:

10.2.1.1 the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Agreement (including this Addendum); and

10.2.1.2 if required under Applicable Privacy Laws, the data protection obligations described in this Addendum are imposed on the Subprocessor; and

10.2.2 remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

10.3 Opportunity to Object to Subprocessors. When DEEPQ engages any New Subprocessor during the Term, DEEPQ will, at least 30 days before the New Subprocessor starts processing any Customer Data, notify You of the engagement (including the name, location and activities of the New Subprocessor).

[New Subprocessor]

Name: Google (that is, Google Asia Pacific Pte. Ltd., based in Singapore)

Address: 8 Marina Boulevard, #05-02, Marina Bay Financial Centre, Singapore 018981.

Contact number: +65-65218000

Description of processing: Google provides Google Cloud Platform on which DeepQ AI Platform was built up. Google also provides Google cloud SQL database hosting services.

11 Data Protection Team; Processing Records

11.1 Data Protection Team. DEEPQ's Data Protection Team will provide reasonable assistance with any Your queries related to processing of Customer Data under the applicable Agreement and can be contacted as described in the Notices section of the applicable Agreement.

11.2 Requests. During the Term, if DEEPQ' receives a request or instruction from a third party purporting to be a controller of Customer Personal Data, DEEPQ will advise the third party to contact You.

12 Notices

Notices under this Addendum (including notifications of any Data Incidents) will be delivered to the Notification Email Address. You are responsible to ensure that Notification Email Address remains current and valid.

13 Interpretation

13.1 Precedence. To the extent of any conflict between: this Addendum and the remainder of the Agreement, this Addendum will prevail.

13.2 For clarity, if You have more than one Agreement, this Addendum will amend each of the Agreements separately.

13.3 Section References. Unless indicated otherwise, section references in any Appendix to this Addendum refer to sections of the General Terms of the Addendum.

Exhibit II

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) You, as the user of DeepQ AI Platform (hereinafter "**entity/ies**") transferring the personal data, as listed in **Annex I.A**. (hereinafter each "**data exporter**"), and

(ii) DEEPQ TECHNOLOGY CORP., receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in **Annex I.A**. (hereinafter each "**data importer**")

have agreed to these standard contractual clauses (hereinafter: "**Clauses**").

(c) These Clauses apply with respect to the transfer of personal data as specified in **Annex I.B**.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in **Annex I.B**.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing **Annex I.A**.

(b) Once it has completed the Appendix and signed **Annex I.A**, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in **Annex I.A**.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in **Annex I.B**, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in **Annex II** and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in **Annex I.B**. After the end of the provision of the processing services, the data importer shall, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so. Until the data is deleted, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "**personal data breach**"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in **Annex I.B**.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "**onward transfer**") if the third party is or agrees to be bound by these Clausesor, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable prior notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in **Annex I.B**., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational

measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "**sensitive data**"), the data importer shall apply the specific restrictions and/or additional safeguards set out in **Annex I.B**.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "**onward transfer**") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) **GENERAL WRITTEN** AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) **GENERAL WRITTEN AUTHORISATION** The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in **Annex II** the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in **Annex II** the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its commercially reasonable efforts to resolve the issue amicably in

a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [**Where the data exporter is established in an EU Member State:**] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in **Annex I.C**, shall act as competent supervisory authority.

[**Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:**] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in **Annex I.C**, shall act as competent supervisory authority.

[**Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:**] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in **Annex I.C**, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental

rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its commercially reasonable efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its commercially reasonable efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its commercially reasonable efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the

documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of England and Wales. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.]

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of London.

(b) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(c) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s):

1. Name:
   You, a user of DeepQ AI Platform
2. Adresss or E-mail Address:
   Referred to the contact information You provided to DeepQ
3. Contact person's name, position and contact details:
   Referred to the contact information You provided to DeepQ
4. Activities relevant to the data transferred under these Clauses:
   Upload to DeepQ AI Platform or provide DeepQ with the images which may contain peronal data for the purpose of AI model training and deployment
5. Role:
   Controller or processor, as the case may be

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name:
   DeepQ Technology Corp.
2. Address:
   13F., No. 207-5, Sec. 3, Beixin Rd., Xindian Dist., New Taipei City 231, Taiwan
3. Contact person's name, position and contact details:
   Data Protection Officer, global-privacy@DEEPQ.com
4. Activities relevant to the data transferred under these Clauses:
   Process the images which may contain peronal data You uploaded to DeepQ AI Platform or provided with DeepQ soely on Your instruction. The data processing may include deleting the images, changing the format of the images, and other forms of processing.
5. Role :
   Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred: as shown in the images uploaded or provided by data exporter.

Categories of personal data transferred: as shown in the images uploaded or provided by data exporter.

Sensitive data transferred (if applicable) and applied restrictions or safeguards: only authorized personnel and third party service providers are permitted access to personal information, and that access is limited by need.

The frequency of the transfer: the data is transferred on an one-off basis.

Nature of the processing: data hosting and database solution.

Purpose(s) of the data transfer and further processing: for data hosting and database solution provided by selected third party service providers.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: the data will be retained (i) within the term where the data exporter remain as a licensed user of the DeepQ AI Platform and (ii) one (1) year after such license to use has expired or been terminated for the purpose of DeepQ continuing its proper management and administration.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: data will be transferred to selected third party service providers for the pirpose of data hosting and database solution. The data will be retained (i) within the term where the data exporter remain as a licensed user of the DeepQ AI Platform and (ii) one (1) year after such license to use has expired or been terminated for the purpose of DeepQ continuing its proper management and administration.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

[Where the data exporter is established in an EU Member State:] the supervisory authority of the EU Member State in which the data exporter is established.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] the supervisory authority of the EU Member State where the data exporter's representative is established.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] the supervisory authority of one of the EU Member State in which the data subject(s) is located.

……

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

- Measures of pseudonymisation and encryption of personal data:
  Has been complied with DeepQ Security document *S-G20-03 Information Asset Category and Group, S-O21Encrpytion Management Process*

- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services:
  Has been complied with DeepQ Security Document *S-O19-01, Disaster Recovery Plan, S-O19-02 Disaster Recovery Drill Report*

- 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:
  Has been complied with DeepQ Security Document *S-O19-01, Disaster Recovery Plan, S-O19-02 Disaster Recovery Drill Report*

- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing:
  Has been complied with DeepQ Security Document *S-G18 Information System Acquisition Development and Maintenance Guidelines*

- Measures for user identification and authorization:
  Has been complied with DeepQ Security Document *S-O06 Account Management Process*

- Measures for the protection of data during transmission:
  Has been complied with DeepQ Security Document *S-G20-03 Information Asset Category and Group, S-O21Encrpytion Management Process*

- Measures for the protection of data during storage:
  Has been complied with DeepQ Security Document *S-G20-03 Information Asset Category and Group, S-O21Encrpytion Management Process*

- Measures for ensuring physical security of locations at which personal data are processed:
  Has been complied with DeepQ Security Document *S-O02 Physical Security Process*

- Measures for ensuring events logging
  Has been complied with DeepQ Security Document *S-O12 Log Management Process*

- Measures for ensuring system configuration, including default configuration
  Has been complied with DeepQ Security Document *S-G18 Information System Acquisition Development and Maintenance Guidelines*

- Measures for internal IT and IT security governance and management:
  Has been complied with DeepQ Security Document *S-O07 System Operation Process, S-O04 Network Security Management Process*

- Measures for certification/assurance of processes and products:
  Has been complied with DeepQ Security Document *S-O16 Application Development and Deployment Security Process*

- Measures for ensuring data minimization:
  Has been complied with DeepQ Security Document *P-G06 Personal Information Processing Guideline*

- Measures for ensuring data quality
  Has been complied with DeepQ Security Document *P-G06 Personal Information Processing Guideline*

- Measures for ensuring limited data retention:
  Has been complied with DeepQ Security Document *P-G06 Personal Information Processing Guideline*

- Measures for ensuring accountability:
  Has been complied with DeepQ Security Document *S-G20 Information Asset Management Guideline, S-G02 Security Operation Guidelines*

- Measures for allowing data portability and ensuring erasure:
  Has been complied with DeepQ Security Document *P-G13 Data Subject Rights Exercise and Management Guideline, S-O05 Data Handling Process*

For transfers to (sub-) processors, also describe the specific technical and organisational 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

1. Google: https://cloud.google.com/security

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

The controller has authorised the use of the following sub-processors:

1. Name: Google (that is, Google Asia Pacific Pte. Ltd., based in Singapore)
   Address: 8 Marina Boulevard, #05-02, Marina Bay Financial Centre, Singapore 018981.
   Contact number: +65-65218000
   Description of processing: Google provides Google Cloud Platform on which DeepQ AI Platform was built up. Google also provides Google cloud SQL database hosting services.

Exhibit III

Business Associate Agreement

Definitions

Catch-all definition:

The following terms used in this Business Associate Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean **DEEPQ TECHNOLOGY CORP**.

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean **You, as a user of DeepQ AI Platform**.

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the covered entity as necessary to satisfy covered entity's obligations under 45 CFR 164.524;

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

(g) Maintain and make available the information required to provide an accounting of disclosures to the covered entity as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information as necessary to perform the services set forth in this Agreement or User Terms. Business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c) only for providing services pursuant to this Agreement or User Terms.

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information consistent with covered entity's minimum necessary policies and procedures.

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity except for the specific uses and disclosures set forth below.

(e) Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

Permissible Requests by Covered Entity

Except as otherwise provided herein, covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity.

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of these User Terms coming into effect, and shall terminate upon these User Terms ceasing to apply between covered entity and business associate or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement and business associate has not cured the breach or ended the violation within 2 month upon notification of such breach or violation by covered entity.

(c) Obligations of Business Associate Upon Termination.

Except as otherwise provided herein, after one (1) year of termination of this Agreement for any reason, business associate shall destroy all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

If applicable, upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

(i) Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
(ii) Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;

(iii) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;

(iv) Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate" which applied prior to termination; and

(v) Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous

(a) Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

DeepQ AI 平台使用條款

更新日期: 2024 年 02 月 20 日

感謝您使用 DeepQ AI 平台（「**本平台**」）。請仔細閱讀 DeepQ AI 平台之使用條款（「**本條款**」）以及本使用條款中所包含的其他條款（「**其他條款**」，「**本條款**」及「**其**

他條款」合稱為「**本使用條款**」），以了解您的權利和責任。透過使用本平台或存取本平台所提供之產品或服務，您同意接受本使用條款之約束。若您不同意本使用條款之任何內容，請勿使用或存取本平台之任何產品或服務。

您了解本使用條款可能不定期修改，修改後的使用條款將透過本平台軟體更新的方式提供或在 DeepQ 的網站上公告。如您於使用條款修訂通知或公告過後仍繼續存取或使用本平台之產品或服務，即表示您接受並同意修訂之條款。您應於每次存取或使用本平台所提供之產品或服務時查看本使用條款，俾以隨時了解任何與您相關的條款變更。若本使用條款與其他條款間有衝突或不一致，以其他條款為準。

1. **DeepQ AI 平台**。本平台是由奧啓迪科技股份有限公司（「**本公司**」、「DeepQ」）所開發和營運的機器學習平台，提供使用者機器學習的模型訓練環境，使用者可將其資料集（dataset）透過平台管理介面上傳至本平台，以進行機器學習模型訓練或資料標註（annotation）（以下稱「**本服務**」）。您所上傳的資料集稱為「**使用者資料**」。

2. **最低年齡**。本平台的服務是提供給年滿 16 歲以上（且於使用者所在地區使用者已達法定成年人年齡）的使用者使用。您擔保您在使用本平台時，您已經年滿 16 歲（且於您所在地區您已達法定成年人年齡）。若您的年齡小於 16 歲、或於您所在地區您尚未達法定成年人年齡或您的法律行為仍須得到您父母之同意，您必須取得您的父母或法定代理人之許可，並與父母或法定代理人一同審閱本使用條款，確保您和您的父母或法定代理人理解並同意本使用條款。

3. **設立帳戶**。為使用本平台的特定功能，您必須在本平台上註冊帳戶，若您在本平台註冊的帳戶是由您所屬雇主或組織授權給您使用，您除了應遵守本使用條款外，亦應遵守您所屬雇主或組織所規定之帳戶使用規範。您必須保護好您的登入憑證，不要授權或與任何第三方分享使用它。一旦您或您代表您的雇主或組織在本平台上註冊帳號，您或您的雇主或組織必須就以您或您的雇主或組織的帳號所進行的一切活動負責。若您懷疑您的帳號未經您授權而被第三方盜用，您必須立即通知您所屬雇主或組織的系統管理者。若您為組織管理員，您享有為組員設定帳號之權限；為組

員設定帳號時，您擔保您已取得組員之同意而得合法使用其 email 等資料進行帳號設定。

4. **系統需求。**為使用透過本平台所提供之服務，您將需要一台連接網路的電腦、網際網路連線及其他相容的軟體。您了解這些系統需求規範可能不定時變更，並可能影響您對本服務的使用。您應就這些系統需求和相關費用 (例如網路費) 自行負責。

5. **本平台服務內容**
    a. 本平台是一機器學習模組管理服務平台，您可以透過本平台上傳您所要進行機器模型訓練或資料標註的使用者資料。您可以透過本平台的管理頁面管理您所上傳的使用者資料。若您於使用本平台時遇到問題 (例如，使用者資料無法上傳、或請求 DeepQ 協助刪除使用者資料)，請您與 DeepQ 聯繫，DeepQ 將提供必要協助，包括但不限於使用者資料上傳測試及轉檔、刪除使用者資料等。
    b. 本平台可能提供給上傳資料集之管理者可邀請第三方參與模型訓練或資料標註之工作專案（包括本平台所提供之其他機器學習訓練工具）的功能（下稱「**工作專案**」）。如果您邀請第三方參與您的工作專案，您必須自行決定並管理第三方在工作專案中的角色及權限，您應就這些第三方權限管理負全部責任。你應使被邀請參與工作專案之第三方遵守資料集擁有者所賦予之權限。
    c. 本平台僅提供機器學習管理環境，DeepQ 對於您所上傳的使用者資料之正確性、合法性、完整性不提供任何保證，您應確保您所上傳的使用者資料內容、和使用者資料的處理利用符合相關法令規定（包括但不限於個人資料保護相關法令），並且就您所上傳的使用者資料之正確性、合法性、完整性自行負完全的責任。
    d. **您應避免上傳帶有個人資料之一切資料到本平台或將該等資料提供給 DeepQ**，否則將依第 18 條「賠償義務」規定決定您的責任；如果您所上傳的資料可能包含個人資料，您應確保您或您所屬的雇主或組織已經取得該個人資料主體的書面同意，並且已依照相關法令或標準(特別是關於蒐集個人資料主體之個人資料之規定) 處理。對於您所上傳的使用者資料，若是 DICOM 檔案格式，經本平台偵測到其標籤欄位含有足以識別個人之資料

（例如以元資料形式顯示之姓名及 ID）者，本平台得依其自身判斷於處理前去除該被偵測之元資料，但 DeepQ 並不保證 DICOM 檔案標籤欄位所有的可識別個人資料均可完全去除。

e. 若您上傳帶有他人個人資料之一切資料至本平台或將其提供給 DeepQ，您與 DeepQ 間之關係將視情況另受**附錄 I** 資料處理附件、**附錄 II** 標準契約條款及**附錄 III** 商業夥伴協議之拘束。請至相關附錄參閱詳細條款內容。**附錄 I**、**附錄 II** 及**附錄 III** 之之適用規則如下：(i) 若您與 DeepQ 間之關係適用 GDPR 規定、且涉及 GDPR 所稱之跨境傳輸時，優先適用**附錄 I** 及**附錄 II** 之規定；(ii) 若您與 DeepQ 間之關係適用 GDPR 規定，但不涉及跨境傳輸，優先適用**附錄 I** 之規定；(iii) 若您與 DeepQ 間之關係適用 HIPAA 規定時，優先適用**附錄 III 之**規定；(iv) 若您與 DeepQ 間之關係既不適用 GDPR 規定亦不適用 HIPAA 規定，優先適用**附錄 I** 之規定。若您與 DeepQ 間之關係適用 GDPR 及 HIPAA 以外之隱私及資安法令，則**附錄 I** 之歐盟規則第 2016/679 號及 2018/1725 號、及**附錄 II** 之 45 CFR 160.103 之規定 (於適當且該所適用之隱私及資安法令允許之範圍內) 將被所應適用之隱私及資安法令所取代。

f. 您應擔保上傳之一切資料之取得及使用之合法性，如有違反法令之情事，您應自負一切責任。

g. 除了本平台使用條款或隱私權聲明另有規定、或經您所屬雇主或組織（即與 DeepQ 簽署授權合約之客戶）同意外，DeepQ 不會檢視、收集、處理或與第三方分享您所上傳、提供或輸入的一切資料（包括使用者資料）。惟如 (i) 基於法律規定或主管機關要求、(ii) 保護本平台之資訊安全、改進系爭平台的功能或服務品質、或為處理您的技術支援需求，DeepQ 可能需要存取、檢視您的標註資料或所上傳的使用者資料。

h. 您只可於使用/試用期間內在本平台上依本使用條款規定之方式使用服務成果（指您因使用本服務所獲致之一切成果，稱為「**服務成果**」，包括但不限於訓練所得之機器學習模型）。

6. **數據備份及資料銷毀。**本平台不提供數據備份託管服務，(i) 本公司不保證您所上傳的使用者資料不會受到移除、破壞、毀損、遺失或不存在；(ii) 您應自行定期就您所上傳至本平台的使用者資料、及您透過本平台使用服務所得到的資訊進行備

份。本使用條款終止、或使用/試用期間結束後，本公司將依內部程序銷毀你所上傳之使用者資料；若您希望保留你所上傳之使用者資料，請您於本使用條款終止、或使用/試用期間結束前以書面通知本公司，本公司將盡快與您聯繫協商資料保管合約事宜。

7. **許可。**在您完全遵守本使用條款之前提條件下， 本公司授與您有限的、個人的、不可轉讓的、非獨佔的、可撤銷的權利，供您在您所適用的試用、租借、購買或授權期間內、或本公司有權提供服務予您的期間內，以**個人和非商業用途方式**使用本公司所控制營運的本平台、服務和服務成果。**本平台、服務和服務成果不得用於臨床試驗、不得基於醫療目的或商業化目的而使用、不得以任何非本使用條款允許之方式使用**。

8. **授權限制。**若您違反本使用條款，本公司得在不退款的情況下，立即終止您使用本平台、本服務、服務成果、產品、和/或本公司關聯帳戶的權利。本使用條款第 7 條等所授與的權利，係以您遵守下列規定為前提，您不得：
    a. 規避本平台中的任何技術限制，或使用本平台時試圖或結合任何用於規避技術限制之裝置、程式或服務，以規避或破壞用於控制存取本平台之技術限制；
    b. 還原工程、解編、破解、反向組譯或以其他方式試圖存取與本平台相關的原始碼，但相關法律明文允許者，不在此限；
    c. 未經授權將任何本平台上軟體、演算法或您擁有的使用本平台權利透過銷售、租賃、出租、再發佈、散播、修改、再授權、轉讓、或移轉方式給任何第三方，但如所適用的終端使用者授權協議另有規定者，不在此限；
    d. 修改任何本平台、服務或服務成果之全部或部分，或作成衍生著作；
    e. 移除本平台、任何服務或服務成果、或其備份的所有權通知或標籤；
    f. 將本平台、任何服務或服務成果用於臨床試驗、或基於醫療目的、商業化目的、及任何非本使用這條款允許之方式使用，但如您或您所屬雇主或組織與 DeepQ 間的終端使用者授權協議另有規定者，不在此限；
    g. 在任何公共場所演出或展示本平台、任何服務或服務成果的全部或部分，無論您是否就您的展出收費，該等演出或展示均是禁止的，但如您或您所屬雇主或組織與 DeepQ 間的終端使用者授權許可協議另有規定者，不在此限；

h. 使用本平台或任何本平台所提供之服務、或服務成果侵害本公司及其關係企業或任何第三方的權利，或以違反任何相關法律或任何適用終端使用者授權協議的方式使用本平台、任何本平台所提供之服務、或服務成果；
i. 在本平台上使用任何自動化工具進行與機器學習訓練無關的活動，例如探索外部網站弱點、惡意攻擊其他網站、試圖以不當方式竄改、破壞、企圖掃描本服務或干擾其他使用者；或
j. 以本使用條款未允許的方式使用本平台、任何本平台所提供之服務或服務成果。

9. **支援和更新。**除了本使用條款規定內容，本公司沒有義務、且可能不會就本平台或任何透過本平台發佈之服務、服務成果提供任何支援服務。

10. **隱私權。**為使用本平台或透過本平台所發佈的服務之特定功能，可能要求您提供某些個人資訊，包括您的姓名、您的註冊帳號所使用的 email 及密碼。本公司將依照本平台之隱私權聲明，收集、處理並儲存您使用本平台時所提供的個人資料及保護您的隱私權。請您詳細閱讀本平台之隱私權政策。

11. **可接受的使用政策**
    a. 您同意您不會不當使用或試圖不當使用本平台，包括但不限於任何違反 DeepQ 行為準則。
    b. 若本公司認為有違反本使用條款之情事， 本公司可能會採取法律行動，與司法單位合作並提起訴訟。除非所適用法律另有禁止規定外，您同意與本公司合作，調查您或其他人可能之違反行為。您授權本公司安裝、採用、管理和施行一種或多種軟體、監控措施，或採取其它方式以確認違法活動或違反本使用條款之行為，或追蹤本公司認為可能的違法活動或違反本使用條款之行為。

12. **智慧財產權所有權。**
    a. 除非本使用條款、或您或您所屬雇主或組織與 DeepQ 間的終端使用者授權許可協議另有規定外，本公司及其關係企業、授權第三方和供應商擁有本平台、透過本平台所提供之服務、及服務成果之所有權、智慧財產權和其他專

屬權利，並且保留所有未在本使用條款中明確授予您的任何權利。DeepQ 相關標誌、和本平台中其他 DeepQ 產品及服務之名稱，均為 DeepQ 及其關係企業的商標或標誌。此外，任何與本平台或透過本平台所發佈產品或服務相關的其他第三方公司名稱、產品名稱、服務名稱及標誌，可能為其他第三方所擁有的商標或標誌，未經其允許不得使用。

b. 本平台可能包含受開放原始碼或第三方授權條款（「**第三方條款**」）規範的第三方軟體，您對該第三方軟體的使用，應受到其所含任何第三方條款的限制。你可以在本平台的設定頁面進一步了解這些第三方軟體以及其所適用的第三方條款。

13. **反饋。**除了您依本使用條款所上傳之使用者資料外，您可能提供口頭或書面的評論、建議、想法、計畫、說明、繪圖或其它關於與本平台或產品相關的資訊（「**反饋**」）。本公司有權在對你不負任何責任之前提下使用、揭露、複製、授權或散佈上述反饋。

14. **終止。**如您違反本使用條款之任何規定，本使用條款將自動終止。您可以隨時透過取消您的帳號而終止本使用條款。您了解您不會因為本使用條款的終止而獲得任何退款，包括任何與訂購方案相關之費用。當本使用條款、服務或試用服務終止、或使用/試用期間屆至，您必須立即停止繼續使用本平台，惟下列使用條文將繼續有效：第 5 條第(d)項前半段、第 5 條第(e)項 (視情況繼續有效)、第 5 條第(f)項、第 7 條後段、第 8 至 26 條。本公司保留隨時未經事前通知您，改變、移除、刪除、限制或禁止使用、或停止提供您就本平台或任何服務全部或一部之權利或授權。

15. **免責聲明。**在相關法律許可最大範圍內，本平台、所有透過本平台所提供的服務是「依現況」、「現有」之條件提供給您，本公司不保證「無瑕疵」，相關使用和效能風險概由您自行承擔。本公司及其供應商和授權人不提供任何明示、默示或法定之聲明、保證或條件，且在此排除任何可銷性、適售品質、符合特定目的、所有權、無權利瑕疵或未侵權之任何默示擔保。本公司、其供應商和授權第三方尤其**不保證**本平台、透過本平台所提供之服務：(I) 可符合您的需求或能與任何第三方軟體、應用程式或第三方硬體搭配運作；(II) 能夠不間斷、即時、安全或毫無錯誤地進行運作；(III) 透過其取得的任何資訊或內容均為正確、完整或可靠；或 (IV) 其中

的瑕疵或錯誤均能被更正。您透過本平台所使用之服務和您於本平台下載或使用之其他資料，使用等風險均由您自行承擔，且您必須自行負責因此產生的任何損害或損失。本平台的使用可能會影響第三方硬體、軟體、應用程式、裝置或服務。您了解您可能擁有依照當地法令規定不得以合約變更之其他權利。尤其，如當地法令有規定不得以合約排除之法定條款，該等條款將視為納入本使用條款，但本公司對違反該等法定條款的責任僅限於該項法律許可的範圍。

16. **特定損害免責聲明。**本公司、供應商或授權第三方對於任何因本使用條款、或本平台、或任何透過本平台所提供之服務所生或與之相關的衍生、特殊、意外、直接、間接或懲罰性損害；或利潤、業務、商譽、預期收入、或使用的損失；或數據、保密資訊或其它資訊的滅失或損壞；營運中斷、人身傷害、財產損失，隱私權受侵害，或未能履行誠信和合理關照之責任、過失及任何其它金錢或損失類型，均不負任何責任。即使本公司、供應商或授權第三方已被告知造成此類損失之可能性，亦同。

部分司法管轄區不允許排除或限制故意行為（包括詐欺、欺詐性不實陳述以及未揭露瑕疵情況）、產品責任或人員傷亡導致之衍生性或附帶性損害、損失或責任。本第 16 條不得被解釋為排除該等司法管轄區相關法律規定不得以合約排除之責任。若您居住於該等司法管轄區或受當地法律所拘束，您所享有之任何法定權利將僅限於該法律許可之範圍（如果有的話）。若法律規定不得以合約限制，則本第 16 條所述限制與排除將不適用於您。

17. **責任限制與唯一救濟。**在所適用的法律允許的最大範圍內，及在第 16 條未排除或免責的範圍內，本公司、其供應商和授權第三方就您因本使用條款、本平台、透過本平台所提供之服務、及服務成果所生或任何相關之損害、人身傷害和損失，應向您所負擔的累計責任總額，同時也是您於本使用條款的唯一救濟，應以以下方式計算責任總額：賠償您基於合理地信賴本平台、透過本平台所提供之服務、及服務成果所造成的實際損失，且以五美元（US$5.00）為上限。

即使有多數針對因本使用條款、本平台、透過本平台所提供之服務、服務成果、或支援的提供或不提供，所提出的主張或訴訟，亦不會擴大或延伸前述金錢賠償範

圍。除本條第三段所述救濟外，此等實際金錢損害賠償將是您的唯一救濟。

部分司法管轄區不允許排除或限制故意行為（包括詐欺、欺詐性不實陳述以及未揭露瑕疵）、產品責任或人員傷亡導致之衍生性或附帶性損害、損失或責任。本第 18 條不得排除該等司法管轄區相關法律規定不得以合約排除之責任。若您居住於該等司法管轄區或受當地法律所拘束，您所享有之任何法定權利將僅限於該法律許可之範圍（如果有的話）。若規定不得以合約限制，則本第 17 條所述限制與排除將不適用於您。

除了所適用法律另有強制規定，您及本公司均同意在爭議發生後的一 (1) 年內應提出請求或主張，否則該請求或主張永久遭到禁止（亦即您及本公司將無權繼續針對該爭議提出請求或求償）。

18. **賠償義務。**若有任何第三方主張 (i) 您未經授權或未依照授權方式使用本平台、透過本平台所提供的服務及服務成果；(ii) 您違反本使用條款；(iii) 您侵害他人權利或違反相關法律；(iv) 您所提供的任何使用者資料，而對本公司及其董事、主管、員工、代理人、合作夥伴、供應商和授權人索賠或要求，您應使前述對象免於損害、並賠償其因此所生之損害（包括合理之律師費）。

19. **限制使用。**本平台、透過本平台所提供的服務及服務成果並非供您使用於不需要有故障安全防護（fail-safe）之系統。如可預見在某些裝置或系統中使用本平台、透過本平台所提供之服務，因故障可能造成人員受傷或死亡之風險，則您不得於該等裝置或系統中使用，例如不得於用於核能設備、航空器導航或通訊系統，和航空交通管制。

20. **紛爭解決準據法及司法管轄區。**除本使用條款另有約定外，本使用條款之解釋或任何違反本使用條款所衍生的爭議或糾紛，均以台灣之法律作為準據法，惟不適用法律衝突原則。所有其他糾紛包含依消費者保護法、不當競爭法和侵權行為所生之糾紛或主張，應以您居住國家或地區的法律作為準據法。除本使用條款另有約定外，針對因本使用條款或其相關事宜所引起之任何爭議，您不可撤銷地同意，因本使用

條款所生之任何爭議或糾紛，應以臺灣臺北地方法院為第一審法院。若所適用的法律不允許指定台北地方法院為第一審法院，則依相關法律規定決定管轄法院。

21. **法律效力。**若您居住所在國家或地區法律並未允許透過法律方式變更您的權利，則本使用條款概不變更您依居住地法律享有的權利。您依居住所在國家法律享有的權利，得附加至本使用條款權利。

22. **法律遵循及出口規定：**您應遵守本平台、任何透過本平台發佈之服務及/或服務成果所適用的所有國內或國際法律、規則和法規，包括但不限於美國出口管理法規（Export Administration Regulations）（軟體需受該法規拘束），以及政府所頒布之相關使用者、使用用途及目的地之限制。

23. **一般條款。**本使用條款中之條款標題僅供各方當事人方便使用，不具備法律或合約之意義。本公司若未針對您的相關違約行為採取行動，並非代表其拋棄針對後續或類似相關違約行為採取行動之權利。除非以書面方式簽署，否則本使用條款之任何條款之拋棄均為無效，任何棄權均不得視為對相同條款或其他條款之棄權。若具有充分管轄權之法院裁定本使用條款之任何條款或限制為非法、無效或無法執行時，其餘條款或限制仍具有完整之效果及效力，任何方面均不受影響、削弱或廢止。您不得依照本使用條款轉讓、移轉或轉授權您的權利（若有的話）。本使用條款對所有本公司之繼任者及受讓人皆具有約束力。

24. **完整合約。**除您或您所屬雇主或組織與 DeepQ 間的終端使用者授權許可協議另有規定者，本使用條款構成就本平台、任何透過本平台發佈之服務及/或服務成果之授權及使用的完整合意。

25. **聯絡資訊。**如果您對本使用條款有任何問題，請將所有通知及信件傳達至：

奧啓迪科技股份有限公司

收件者：資料保護官

中華民國台灣

231 新北市新店區北新路 3 段 207 之 5 號 13 樓

附錄 I

資料處理附錄

您使用 DEEPQ 提供之特定服務及產品時可能涉及個人資料之處理，於個別合約 (以下合稱為「**合約**」) 闡明 DEEPQ 的角色為您的資料處理者時，將適用本資料處理附錄 (包含其附件，以下合稱為「**本附錄**」) 之規定。

一般條款

1. 總覽

本附錄內容說明雙方當事人之義務，包括於所應適用之隱私、資訊安全、及資料保護法令下，與客戶資料 (定義參後述) 有關之資料處理及資訊安全義務。本附錄自「附錄生效日」(定義參後述) 生效，且將取代先前適用於客戶資料之資料處理及資訊安全之條款。本附錄所使用之專用語以合約中所賦予之定義為準。

2. 定義

2.1 於本附錄中：

2.1.1「附錄生效日」指(a) 您接受本附錄條款時；(b) DEEPQ 提供相應服務時；(c) 雙方當事人另行同意之日期 (以較早者為準)。

2.1.2「所應適用之隱私法律」指適用於客戶個人資料之處理的任何國家、聯邦、歐盟、州級、省級或其他隱私、資訊安全、或資料保護法令或法規。

2.1.3「合規認證」之定義依第 6.4 條約定。

2.1.4「客戶資料」之定義以合約中所賦予之定義為準。

2.1.5「客戶個人資料」指客戶資料中所包含之個人資料，包括所應適用之隱私法律中所定義之任何特種個人資料或敏感性個人資料。

2.1.6「資訊安全事件」指 DEEPQ 之資訊安全發生事故所導致存放於 DEEPQ 運營或控制之系統中之客戶資料受到意外或非法地破壞、丟失、竄改、未經授權之揭露、接觸。

2.1.7「歐盟一般資料保護規則 (EU GDPR)」指歐洲議會及歐盟理事會 2016 年 4 月 27 日關於自然人個人資料處理及自由流動之保護的歐盟規則第 2016/679 號 (該規則廢除 95/46/EC 指令)。

2.1.8「歐洲資料保護法」包含 (依適用情形) (a)一般資料保護規則 (GDPR)；(b) 瑞士之資料保護聯邦法令 (Swiss FADP)。

2.1.9「歐洲法令」指 (依適用情形) (a) 歐盟或歐盟成員國法 (若歐盟一般資料保護規則 (EU GDPR) 適用於客戶個人資料之處理)；(b) 英國法或部份之英國法 (若英國一般資料保護規則 (UK GDPR) 適用於客戶個人資料之處理)；(c) 瑞士法 (若瑞士資料保護聯邦法令 (Swiss FADP) 適用於客戶個人資料之處理) 。

2.1.10「一般資料保護規則 (GDPR)」指 (依適用情形) (a) 歐盟一般資料保護規則 (EU GDPR)；或 (b) 英國一般資料保護規則 (UK GDPR)。

2.1.11「DEEPQ 的第三方稽核人員」指由 DEEPQ 指派之合格、獨立第三方稽核人員，DEEPQ 將向您揭露該稽核人員之身分。

2.1.12「您的指示」之定義依第 5.2 條約定。

2.1.13「通知電子郵件地址」指您於合約中所指定之電子郵件地址，或您以書面指定用於接收 DEEPQ 發送之特定通知之電子郵件地址。

2.1.14「資訊安全文件」指合規認證。

2.1.15「資訊安全措施」之定義依第 6.1.1 條約定。

2.1.16「服務」之定義以合約中所賦予之定義為準。

2.1.17「委外廠商 (Subprocessor)」指資料處理者 (processor) 為提供服務，而授權第三方以另一名資料處理者之身分處理客戶資料，該第三方即為委外廠商。

2.1.18「監管機關」指 (依適用情形) (a) 歐盟一般資料保護規則 (EU GDPR) 所定義之監管機關 (supervisory authority)；(b) 英國一般資料保護規則 (UK GDPR) 或瑞士資料保護聯邦法令 (Swiss FADP) 所定義之委員 (Commissioner)。

2.1.19「瑞士資料保護聯邦法令 (Swiss FADP)」指 (依適用情形) 1992 年 6 月 19 日瑞士資料保護聯邦法令或 2020 年 9 月 25 日修正版瑞士資料保護聯邦法令 (及 2022 年 8 月 31 日資料保護聯邦條例)。

2.1.20「服務期間」指自附錄生效日至 DEEPQ 完成服務之提供時止，包含 (若可適用) 任何服務中止期間、及終止後 DEEPQ 為交接目的仍繼續提供服務之期間。

2.2 本附錄所使用之「個人資料」、「資料主體」、「資料處理」、「資料控制者」及「資料處理者」之定義以所應適用之隱私法律所賦予之定義為準；若此等所應適用之隱私法律不存在，則以歐盟一般資料保護規則 (EU GDPR) 所賦予之定義為準。

2.3 「資料主體」、「資料處理」及「資料控制者」，各自包含所應適用之隱私法律所定義之「消費者」「企業」及「服務提供者」。

3. 有效期間

無論所應適用之合約是否終止或屆期，本附錄將持續有效，直至本附錄所示之有效期間屆至時自動終止。

4. 雙方角色；法規遵循

4.1 雙方角色：(依適用情形) DEEPQ 為客戶個人資料之資料處理者，而您為資料控制者；或 DEEPQ 為客戶個人資料之委外廠商，而您為資料處理者。

4.2 法規遵循：任一方於處理客戶個人資料時，應盡所應適用之隱私法律所規範之義務。

5. 資料處理

5.1 若您為資料處理者：

5.1.1 您持續擔保相關的資料控制者已就下列事項給與授權：

5.1.1.1 您的指示；

5.1.1.2 您使用 DEEPQ 作為委外廠商；

5.1.1.3 DEEPQ 使用第 10 條所列之委外廠商；

5.1.2 您應立即將 DEEPQ 依第 6.2.1 條、第 8.2.1 條或第 10.4 條發出之通知，轉發給資料控制者。

5.1.3 您可以將其他任何由 DEEPQ 依本附錄所提供之資訊提供給相關的資料控制者，包括 DEEPQ 的資料中心、或委外廠商之名稱、地點及所從事行為。

5.2 遵循您的指示：您指示 DEEPQ 依所應適用之合約 (包含本附錄) 及相關法令之規定處理客戶資料，此等資料處理只包含下列行為：

5.2.1 提供、確保、監控 DEEPQ 之服務；

5.2.2 根據下列方式所確定之行為：

5.2.2.1 您對服務之使用；及

5.2.2.2 其他由您給予並經 DEEPQ 依本附錄認可之書面指示 (以上合稱「您的指示」)。

5.3 除非 (a) 應適用歐洲資料保護法而歐洲法令禁止，(b) 應適用其他所應適用之隱私法律而我應適用之法律禁止，否則 DEEPQ 將會遵循您的指示。

5.4 除非 DEEPQ 收到資料控制者之進一步指示，否則 DEEPQ 只會基於本附錄所列出之特定目的處理您的個人資料。

6. 資訊安全

6.1 DEEPQ 的資訊安全措施、管控與協助

6.1.1 DEEPQ 的資訊安全措施　DEEPQ 會依附錄 1 所述執行並維持技術、組織及實體措施 (稱「資訊安全措施」)，以防範客戶資料受到受到意外或非法地破壞、丟失、竄

改、未經授權之揭露、接觸。資訊安全措施包含有助於確保持續保密性、完整性及可用性之措施。DEEPQ 有權隨時更新資訊安全措施，前提是這些更新不會大幅降低服務的安全性。在評估適當的安全等級時，雙方應適切考量技術水準、執行成本、資料處理的本質、範圍、情境及目的、及所涉及之資料主體之風險。若資料處理涉及所應適用的隱私法律所指之敏感性個資，DEEPQ 將會採取特定的限制措施及/或額外的安全措施。

6.1.2 接觸權限及合規遵循　DEEPQ 將：

6.1.2.1 授權其員工、分包商及委外廠商，僅可於為遵循指示之極其必要範圍內接觸客戶資料；及

6.1.2.2 確保所有被授權處理客戶資料之人均受保密義務之拘束。

6.1.3 DEEPQ 就資訊安全提供之協助　DEEPQ 將會 (考量處理客戶個人資料、DEEPQ 得接觸之資料之本質) 透過以下方式協助您，以履行您或相關資料控制者 (當您為資料處理者時) 於所應適用之隱私法律下關於資訊安全及個人資料洩漏之義務：

6.1.3.1 執行並維持第 6.1.1 條所示之資訊安全措施；

6.1.3.2 遵循第 6.2 條規定；

6.1.3.3 提供所應適用之合約 (包含本附錄) 所要求之資訊；

6.1.3.4 若上述規定不足以協助您或相關資料控制者履行法定義務，DEEPQ 將依您的要求提供額外的合作及協助。

6.2 資訊安全事件

6.2.1 事件通知　DEEPQ 於知悉資訊安全事件後將即時通知您，並即時採取合理步驟以降低危害並保全客戶資料之安全性。

6.2.2 資訊安全事件之細節　DEEPQ 就資訊安全事件之通知內容包含：資訊安全事件之本質 (包含您受事件影響之資產)、DEEPQ 為處理資訊安全事件及減輕潛在風險而已採取或計畫採取之措施；DEEPQ 建議您為處理資訊安全事件所採取之措施；能向您提供更多資訊之聯繫窗口。若客觀上無法同時提供上述資訊，DEEPQ 之初步通知將納入當時所得獲取之資訊，並在獲取其他資訊時即時提供給您。

6.2.3 DEEPQ 不提供客戶資料評估　DEEPQ 沒有義務評估客戶資料，以滿足特定法律規定關於識別資訊之要求。

6.2.4 DEEPQ 依第 6.2 條就資訊安全事件發出通知或提出反饋，不得被解釋為 DEEPQ 承認其對資訊安全事件有疏失或負有責任。

6.3 您的資訊安全責任與評估

6.3.1 您的資訊安全責任　於不影響 DEEPQ 於第 6.1 條、第 6.2 條、及合約中所應適用之條款所負義務之前提下，關於合約所指服務之使用、及於 DEEPQ 或 DEEPQ 委外廠商之系統以外之處儲存客戶資料之備份，由您自行負責；包括：

6.3.1.1 為確保具備與客戶資料風險相應的資訊安全級別，而使用合約所指服務；

6.3.1.2 確保您用以使用合約所指服務之帳戶驗證憑證、系統及裝置之安全性；

6.3.1.3 適當地備份客戶資料或保留客戶資料之副本。

6.3.2 您的資訊安全評估　您同意，合約所指之服務、資訊安全措施、及 DEEPQ 於本第 6 條所做之承諾，具備與客戶資料風險相應的資訊安全級別 (考量技術水準、實行成本、處理客戶資料之本質、範圍、情境及目的、及對個人造成的風險)。

6.4 合規審查與稽核

6.4.1 您的稽核權利

6.4.1.1 稽核　若所應適用之隱私法律有明文要求，DEEPQ 將會允許您或您所指定之獨立稽核人員依第 6.4.3 條對 DEEPQ 進行稽核，以確認 DEEPQ 是否已盡本附錄所示之義務。於稽核期間，DEEPQ 會依第 6.4 條規定於合理範圍內與您或您所指定之獨立稽核人員合作。

6.4.2 合規審查與稽核之附加商業條款

6.4.2.1 您必須向 DEEPQ 團隊提出第 6.4.1.1 條之稽核要求。

6.4.2.2 DEEPQ 與您將共同討論及事先協議下列事項：合理的開始稽核日期、稽核範圍、持續期間、資訊安全及保密控制措施。

6.4.2.3 DEEPQ 可能針對第 6.4.1.1 條之稽核向您收取費用 (依據 DEEPQ 所生之合理費用)，DEEPQ 會於稽核開始前向您提供費用細節、計算基礎。您所指定之稽核人員進行稽核所生費用將由您自行負擔。

7. DEEPQ 將向您提供合理且必要之資訊，以說明 DEEPQ 已盡本合約下資料處理者之義務。

8. 接觸；當事人權利行使；資料出境

8.1 接觸；更正；限制資料處理；資料可攜性　於服務期間內，DEEPQ 將以符合合約所指服務之方式，使您得接觸、更正客戶資料，限制客戶資料之處理、輸出客戶資料。若您發現客戶個人資料不正確或過時，您應負責以符合合約所指服務之方式，依所應適用之隱私法律規定更正或刪除該等資料。

8.2 當事人權利行使

8.2.1 當事人權利行使下之 DEEPQ 義務　於服務期間內，若 DEEPQ 收到關於客戶個人資料之當事人權利行使請求並提及您，DEEPQ 將：

8.2.1.1 告知資料主體將當事人權利行使請求提交給您；

8.2.1.2 即時通知您；

8.2.1.3 未經您的授權，DEEPQ 不會對當事人權利行使請求作出回應；

8.2.1.4 您負責對此等請求作出回應，包含 (必要時) 以符合合約所指服務之方式回應。

8.2.2 當事人權利行使下 DEEPQ 提供之協助　DEEPQ 將 (考量處理客戶個人資料之本質) 以下述方式協助您履行您或相關資料控制者 (當您為資料處理者時) 依所應適用之隱私法律針對當事人權利行使請求應作出回應之義務：

8.2.2.1 遵循第 8.1 條及第 8.2 條規定；

8.2.2.2 若第 8.1 條及第 8.2 條規定不足以滿足您的法令義務，DEEPQ 會依您的請求向您提供額外的合理協助。

9. 資料處理地點及國際傳輸

9.1 DEEPQ 僅會在資料控制者有書面指示、或 DEEPQ 為了滿足歐盟或歐盟成員國法令對資料處理者要求之義務之前提下，將資料傳輸至第三國或國際組織，並遵循歐盟規則第 2016/679 號或第 2018/1725 號之第五章規定。

9.2 您在此同意，當 DEEPQ 依附錄規定使用委外廠商進行特定的資料處理行為 (以您的名義)，而該資料處理行為涉及歐盟規則第 2016/679 號第五章規定下之個人資料傳輸，則資料處理者及委外廠商得透過簽署歐盟執委會依歐盟規則第 2016/679 號第 46 條第 2 項規定所採納之標準契約條款之方式，以滿足歐盟規則第 2016/679 號第五章規定；前提是得使用該標準契約條款之前提已被滿足。

10. 委外廠商

10.1 同意使用委外廠商　自附錄生效起，您明確授權 DEEPQ 得使用 DEEPQ 之關係企業作為委外廠商，此外，在不影響您於第 10.3 條享有之權利的前提下，您一般性地授權 DEEPQ 得使用其他第三方作為委外廠商 (稱「**新委外廠商**」)。

10.2 使用委外廠商之規定　當使用任何委外廠商時，DEEPQ 會：

10.2.1 確保：

10.2.1.1 委外廠商僅會在執行資料委外處理義務之範圍內依所應適用之合約規定 (包含本附錄) 接觸及使用客戶資料，且

10.2.1.2 若所應適用之隱私法律有所要求時，委外廠商須履行本附錄所述之資料保護義務，且

10.2.2 DEEPQ 對所有委外之資料處理義務、及委外廠商之所有行為及疏失負責。

10.3 賦予您反對使用委外廠商之機會　當 DEEPQ 於服務期間使用任何新委外廠商，DEEPQ 至少會在新委外廠商開始處理客戶資料前 30 日，向您通知 DEEPQ 使用新委外廠商 (包含新委外廠商之名稱、所在地、及新委外廠商將從事之活動)。

【新委外廠商】

名稱：Google (即 Google Asia Pacific Pte. Ltd., 位於新加坡)

地址：8 Marina Boulevard, #05-02, Marina Bay Financial Centre, Singapore 018981.

連絡電話：+65-65218000

資料處理之描述：Google 提供雲端運算服務 Google Cloud Platform，DeepQ AI Platform 建置於 Google Cloud Platform 上。Google 並提供 Google cloud SQL 資料庫代管服務。

11. 資料保護小組；資料處理紀錄

11.1 資料保護小組　針對您關於依所應適用之合約進行客戶資料處理的詢問，DEEPQ 之資料保護小組將提供合理協助，您可透過所應適用之合約中之通知條款內所載資訊聯繫 DEEPQ 之資料保護小組。

11.2 請求　於服務期間內，若 DEEPQ 收到自稱為客戶個人資料之資料控制者所給的請求或指示，DEEPQ 會建議該第三人聯繫您。

12. 通知

依本附錄所發送之通知 (包含資訊安全事件之通知)，應寄送至通知電子郵件地址。您應負責確保該電子郵件地址為最新且有效的。

13. 條款詮釋

13.1 文件適用順序　於本附錄規定及所應適用合約之其他部份規定間有衝突或不一致者，以本附錄規定為準。

13.2 為清楚起見，若您與 DEEPQ 間存在多份所應適用之合約，本附錄將個別增補各該所應適用之合約條款。

13.3 章節參考　除非另有說明，附錄中提及本附錄者，指向的是本附錄的一般條款下之內容。

附錄 1：資訊安全措施

自附錄生效日起，在適用的情況下，DEEPQ 將執行並維持附錄 1 中所應適用之資訊安全措施。

資料處理活動

1. **若 DEEPQ 有權限接觸個人資料：**
    - DEEPQ 使用合理的控制措施以防止對個人資料之非法接觸；
2. **若 DEEPQ 傳輸個人資料：**
    - DEEPQ 將對所有透過網路傳輸之個人資料進行加密；
3. **若 DEEPQ 儲存個人資料：**
    - DEEPQ 將銷毀所有已無使用需要的紙本文件，並保存銷毀此類文件之紀錄；
    - 為儲存及分享個人資料之目的而維持一個安全空間；
    - 通過紀錄每個人的身分，以確保只有參與與資料輸出者合作的特定專案之個人得有權限接觸資料處理者的安全空間，且當該個人之雇傭關係終止、或當該個人不再需要擁有接觸個人資料之權限時，DEEPQ 即會終止該個人之接觸權限。

附錄 II

標準契約條款

第 I 條

第 1 項

目的及範圍

(a) 本標準契約條款係為確保能確實遵守 2016 年 4 月 27 日歐洲議會及歐盟理事會為保護就個人資料移轉至第三國家之自然人個人資料處理與自由流通所制定之歐盟規則第 2016/679 號（個人資料保護規則）。

(b) 本標準契約條款之當事人：

(i) **您**，即 DeepQ AI Platform 之使用者 (以下稱「**公司**」) 且列於**附件 I.A.**之個人資料進行傳輸之自然人/公司/法律實體 (以下稱「**資料輸出者**」)，及

(ii) **奧啓迪科技股份有限公司**，即直接或間接透過其他列於**附件 I.A** 之當事人，自資料輸出者取得個人資料者 (以下稱「**資料輸入者**」)

同意受本標準契約條款 (以下稱「**本條款**」) 拘束。

(c) 本標準契約條款適用於**附件 I.B** 所列之個人資料傳輸。

(d) 附屬於本條款之附件為本條款之一部份。

第 2 項

本條款之效力及不可變更性

(a) 在不變更本條款內容之前提下 (除了選擇適當之模組 (Module(s)) 或增加或更新附件之資訊外)，本條款規範適當的保護措施，包括歐盟規則第 2016/679 號第 46 條(1)條及第 46 條(2)(c) 條所規定之資料主體權利 (data subject rights) 及法律救濟途徑，及歐盟規則第 2016/679 號第 28 條(7) 條涉及資料控制者向資料處理者進行之資料傳輸、標準契約條款。本條款之當事人得將本條款內容納入其合約中，及/或增加其他條款或保護措施；但該條款及保護措施不得直接或間接與本條款衝突，或損及資料主體 (data subject) 之基本權利或自由。

(b) 本條款不影響資料輸出者於歐盟規則第 2016/679 號下所負擔之責任。

第 3 項

第三方受益人

(a) 資料主體得以第三方受益人身分，向資料輸出者及/或資料輸入者行使本條款所示之權利；但不包含以下條款：

(i) 第 1 項、第 2 項、第 3 項、第 6 項、第 7 項；

(ii) 第 8 項- 模組 1：第 8.5 項(e)及第 8.9 項(b)；模組 2：第 8.1 項(b)、第 8.9 項(a)、(c)、(d)及(e)；模組 3：第 8.1 項(a)、(c)及(d)、第 8.9 項(a)、(c)、(d)、(e)、(f)及(g)；模組 4：第 8.1 項(b)及第 8.3 項(b)；

(iii) 第 9 項-模組 2：第 9 項(a)、(c)、(d)及(e)；模組 3：第 9 項(a)、(c)、(d)及(e)；

(iv) 第 12 項-模組 1：第 12 項(a)及(d)；模組 2 及 3：第 12 項(a)、(d)及(f)；

(v) 第 13 項；

(vi) 第 15.1 項(c)、(d)及(e)；

(vii) 第 16 項(e)；

(viii) 第 18 項-模組 1、2 及 3：第 18 項(a)及(b)；模組 4：第 18 項。

(b) 前款規定(a) 不影響資料主體於歐盟規則第 2016/679 號所享有之資料主體權利。

第 4 項

條款解釋

(a) 當本條款使用歐盟規則第 2016/679 號中之用語時，該用語與歐盟規則第 2016/679 號中之用語之意義相同。

(b) 本條款應依歐盟規則第 2016/679 號為解釋依據。

(c) 本條款不得作與歐盟規則第 2016/679 號所規定之權利義務相反之解釋。

第 5 項

適用順序

當本條款與本條款當事人間之契約條款相衝突時，若當事人對該契約條款之合意係發生於本條款生效之後，則應優先適用本條款。

第 6 項

資料傳輸之描述

資料傳輸之細節 (特別是所傳輸的個人資料之種類、資料傳輸之目的) 詳列於**附件 I.B**。

第 7 項

對接條款

(a) 任何第三方於任何時候，經本條款當事人之同意，並填妥及簽署本條款附件及**附件 I.A** 後，即以資料輸出者或資料輸入者身分，受本條款拘束。
(b) 該第三方填妥及簽署本條款附件及**附件 I.A** 後，即成為本條款之當事人，依**附件 I.A** 所示之身分 (資料輸出者或資料輸入者) 於本條款享有權利及負擔義務。
(c) 該第三方不享有或負擔於成為本條款之當事人前已生之權利或義務。

第 II 條-當事人之義務

第 8 項

資料保護措施

資料輸出者擔保，其已盡合理努力確認資料輸入者因執行適當的技術及組織措施而得以盡到本條款所賦予之義務。

模組 2：資料傳輸「控制者」至「處理者」

8.1 指示

(a) 資料輸入者僅得依資料輸出者之書面指示對個人資料進行處理。資料輸出者於本條款有效期間內均得對資料輸入者給予指示。
(b) 若資料輸入者無法遵守資料輸出者之指示，應立即通知資料輸出者。

8.2 目的之限制

除非資料輸出者有進一步指示，否則資料輸入者僅得基於**附件 I.B** 所列之資料傳輸目的處理個人資料。

8.3 透明化

依資料主體之要求，資料輸出者應將本條款 (包含本條款當事人所填妥並簽署之附件) 之複印本無償提供給資料主體。於保護商業祕密及其他機密資訊 (包含**附件 II** 中所描述之技術及組織措施、個人資料) 所必要之範圍內，資料輸出者將前述複印本提供給資料主體前，得先行刪減本條款附件中之部分文字；若資料主體因此無法瞭解刪減後之內容或無法行使其權利，資料輸出者應提供一份有實益的摘要以向資料主體說明。依資料主體之要求，於不揭露刪減內容之範圍內，本條款當事人應向資料主體提供刪減部分文字之理由。本項規定不影響歐盟規則第 2016/679 號第 13 條及第 14 條關於資料輸出者之義務。

8.4 準確性

若資料輸入者知悉其收受的個人資料並不準確或已經過時，應及時通知資料輸出者；資料輸入者應與資料輸出者共同合作刪除或更正該資料。

8.5 資料處理期間、資料刪除或返還

資料輸入者僅能於**附件 I.B** 所示之期間內處理個人資料；資料處理完成後，資料輸入者應代表資料輸出者將所有個人資料刪除，並向資料輸出者確認已完成刪除作業。在資料完成刪除前，資料輸入者應繼續遵守本條款之規定。若資料輸入者所在之當地法令禁止個人資料之刪除，則資料輸入者應保證其會繼續遵循本條款之規定並僅會在當地法令允許之範圍內處理個人資料。本項規定不影響本條款第 14 條之規定，特別是第 14 條(e)關於當資料輸入者於合約期間內有理由相信其受與本條款規定不一致之特定法令或慣例拘束時應通知資料輸出者之規定。

8.6 資料安全

(a) 於資料傳輸時，資料輸入者及資料輸出者應實行適當的技術及組織措施以確保資料安全，包括防範資料安全之違反所導致之意外或非法之資料毀壞、滅失、更改、未獲授權之揭露或存取 (以下稱「**個人資料侵害事件**」)。於評估適當程度之資料安全措施時，本條款當事人應適切考量當前最新技術、實行之成本、資料處理之本質/範圍/背

景事實/目的、資料處理為資料主體所帶來的風險。本條款當事人應特別考量，採行資料加密或假名化 (pseudonymisation) ，包括於資料傳輸時 (若資料處理傳輸之目的在採行該等措施後仍可實現)。於資料假名化時，在可行的前提下，可用以將個人資料連結到特定資料主體之額外資訊應維持由資料輸出者專屬控制。為遵循本條款規定，資料輸出者應至少實行列於**附件 II** 之技術及組織措施。為確保這些措施持續提供適當程度的資訊安全，資料輸入者應執行定期檢視工作。

(b) 資料輸入者於向其員工或人員開放個人資料存取權限時，應限於為實行、管理、監控本條款之執行所嚴格必要之範圍內，資料輸入者並應確保被授予權限處理個人資料之人已承諾保密或受適當的保密義務法規之拘束。

(c) 當資料輸入者依本條款所處理之個人資料發生個人資料侵害事件時，資料輸入者應採取適當措施處理之，包含減輕該事件之負面影響之措施。資料輸入者知悉此等事件後，不得無故拖延而應通知資料輸出者，此項通知應包含資料輸入者之聯絡人資訊(以方便資料輸出者獲取更多資訊)、個人資料侵害事件之本質 (可能包含， 資料主體及個人資料紀錄的種類及概略數量)、可能產生的後果、採行或建議採行之措施 (可能包含，減輕該事件之負面影響之措施)。若資料輸入者不可能同時提供這些資訊，則最初的通知應包含當時可得之資訊，其他進一步的資訊在後續變為可得時，不得無故拖延而應提供給資料輸出者。

(d) 在考量資料處理的本質及資料輸入者可取得之資訊之前提下，資料輸入者應與資料輸出者合作，並協助其遵循其於歐盟規則第 2016/679 號下之義務，特別是通知相關監管機關及受影響之資料主體之義務、

8.7 敏感性資料

當被傳輸的個人資訊會揭露種族、人種、政治意見、宗教或哲學信仰、或貿易聯盟會員身分、基因資料、或用以辨識自然人之生物特徵識別資料、與個人健康或性生活或性傾向有關之資料、與刑事定罪有關之資料 (以下稱「**敏感性資料**」)，資料輸入者應適用**附件 I.B** 中所示之特定限制規定、及/或額外的安全措施。

8.8 後續傳輸

資料輸入者僅能在資料輸出者書面指示下將個人資料揭露給第三方。此外，該資料僅能揭露給位於歐盟以外的第三方 (和資料輸入者位於同一國家、或其他第三方國家，以下稱「**後續傳輸**」)，前提是該第三方同意受本條款拘束 (適用適當之模組條款) ，或

(i) 該後續傳輸係將資料傳輸至歐盟規則第 2016/679 號第 45 條之具備「適當保護程度」之國家；

(ii) 該第三方確保其依歐盟規則第 2016/679 號第 46 條或第 47 條為該資料處理提供適當之安全措施；

(iii) 該後續傳輸是於特定行政、監管、或司法程序下為建立、行使或防禦法律上之請求所必須；或

(iv) 該後續傳輸是為保護資料主體或其他自然人之重要利益所必須。

任何後續傳輸之前提是，資料輸入者須遵循本條款所有其他保護措施，特別是目的限制。

8.9 書面紀錄與條款遵循

(a) 資料輸入者應及時並適切地處理資料輸出者關於本條款下資料處理之詢問。

(b) 本條款當事人應能說明其對本條款之遵循情形，特別是資料輸入者應保存代表資料輸出者進行資料處理活動之適當書面紀錄。

(c) 資料輸入者應向資料輸出者提供所有足以說明其對本條款義務遵循情形之資訊，並在資料輸出者之要求下，每隔一段合理期間或當有跡象顯示未能遵循本條款時，資料輸入者應准許並配合資料輸出者對本條款下之資料處理活動進行稽核。於決定採取審查或稽核時，資料輸出者得考量資料輸入者是否持有相關認證。

(d) 資料輸出者得選擇自行或聘請獨立稽核機關以進行稽核，稽核得包含至資料輸入者之處所或實體設施進行檢視、並應於可行時給予資料輸入者合理之事前通知。

(e) 當相關監管機關要求時，本條款當事人應提供上述(b)/(c)之資訊 (包含稽核結果)。

模組 3：資料傳輸「處理者」至「處理者」

8.1 指示

(a) 在資料處理之前，資料輸出者應向資料出入者告知，資料輸出者為其資料控制者之資料處理者。

(b) 資料輸入者僅得依資料控制者之書面指示 (由資料輸出者所提供)、及資料輸出者之其他書面指示，對個人資料進行處理。資料輸出者之其他書面指示不得與資料控制者之書面指示相衝突。資料控制者及資料輸出者於本條款有效期間內均得對資料輸入者給予進一步指示。

(c) 若資料輸入者無法遵守上述指示，應立即通知資料輸出者。若資料輸入者無法遵守資料控制者之書面指示，資料輸出者應立即通知資料控制者。

(d) 資料輸出者擔保其已將與資料控制者及資料輸出者間之合約、其他雙方所在之歐盟或歐盟成員國之法令所要求之相同資料保護義務加諸於資料輸入者。

8.2 目的之限制

除非資料控制者有進一步指示 (由資料輸出者所提供) 或資料輸出者有進一步指示，否則資料輸入者僅得基於**附件 I.B** 所列之資料傳輸目的處理個人資料。

8.3 透明化

依資料主體之要求，資料輸出者應將本條款 (包含本條款當事人所填妥並簽署之附件) 之複印本無償提供給資料主體。於保護商業祕密及其他機密資訊 (包含**附件 II** 中所描述之技術及組織措施、個人資料) 所必要之範圍內，資料輸出者將前述複印本提供給資料主體前，得先行刪減本條款之附件中之部分文字；若資料主體因此無法瞭解刪減後之內容或無法行使其權利，資料輸出者應提供一份有實益的摘要以向資料主體說明。依資料主體之要求，於不揭露刪減內容之範圍內，本條款當事人應向資料主體提供刪減部分文字之理由。

8.4 準確性

若資料輸入者知悉其收受的個人資料並不準確或已經過時，應及時通知資料輸出者；資料輸入者應與資料輸出者共同合作刪除或更正該資料。

8.5 資料處理期間、資料刪除或返還

資料輸入者僅能於**附件 I.B** 所示之期間內處理個人資料；資料處理完成後，資料輸入者應代表資料輸出者將所有個人資料刪除，並向資料輸出者確認已完成刪除作業。在資料完成刪除前，資料輸入者應繼續遵守本條款規定。若資料輸入者所在之當地法令禁止個人資料之刪除，則資料輸入者應保證其會繼續遵循本條款之規定並僅會在當地法令允許之範圍內處理個人資料。本項規定不影響本條款第 14 條之規定，特別是第 14 條(e)關於當資料輸入者於合約期間內有理由相信其受與本條款規定不一致之特定法令或慣例拘束時應通知資料輸出者之規定。

8.6 資料安全

(a) 於資料傳輸時，資料輸入者及資料輸出者應實行適當的技術及組織措施以確保資料安全，包括防範資料安全之違反所導致之意外或非法之資料毀壞、滅失、更改、未獲授權之揭露或存取(以下稱「個人資料侵害事件」)。於評估適當程度之資料安全措施時，本條款當事人應適切考量當前最新技術、實行之成本、資料處理之本質/範圍/背景事實/目的、資料處理為資料主體所帶來的風險。本條款當事人應特別考量，採行資料加密或假名化 (pseudonymisation) ，包括於資料傳輸時 (若資料處理傳輸之目的在採行該等措施後仍可實現)。於資料假名化時，在可行的前提下，可用以將個人資料連結到特定資料主體之額外資訊應維持由資料輸出者專屬控制。為遵循本條款規定，資料輸出者應至少實行列於**附件 II** 之技術及組織措施。為確保這些措施持續提供適當程度的資訊安全，資料輸入者應執行定期檢視工作。

(b) 資料輸入者於向其員工或人員開放個人資料存取權限時，應限於為實行、管理、監控本條款之執行所嚴格必要之範圍內，資料輸入者並應確保被授予權限處理個人資料之人已承諾保密或受適當的保密義務法規之拘束。

(c) 當資料輸入者依本條款所處理之個人資料發生個人資料侵害事件時，資料輸入者應採取適當措施以處理之，包含減輕該事件之負面影響之措施。資料輸入者知悉此等事件後，不得無故拖延而應通知資料輸出者，此項通知應包含資料輸入者之聯絡人資訊(以方便資料輸出者獲取更多資訊)、個人資料侵害事件之本質 (可能包含， 資料主體及個人資料紀錄的種類及概略數量)、可能產生的後果、採行或建議採行之措施 (可能包含，減輕該事件之負面影響之措施)。若資料輸入者不可能同時提供這些資訊，則最初的通知應包含當時可得之資訊，其他進一步的資訊在後續變為可得時，不得無故拖延而應提供給資料輸出者。

(d) 在考量資料處理的本質及資料輸入者可取得之資訊之前提下，資料輸入者應與資料輸出者合作，並協助其遵循其於歐盟規則第 2016/679 號下之義務，特別是通知相關監管機關及受影響之資料主體之義務。

8.7 敏感性資料

當被傳輸的個人資訊會揭露種族、人種、政治意見、宗教或哲學信仰、或貿易聯盟會員身分、基因資料、或用以辨識自然人之生物特徵識別資料、與個人健康或性生活或性傾向有關之資料、與刑事定罪有關之資料 (以下稱「**敏感性資料**」)，資料輸入者應適用**附件 I.B** 中所示之特定限制規定、及/或額外的安全措施。

8.8 後續傳輸

資料輸入者僅能在資料輸出者書面指示下將個人資料揭露給第三方。此外，該資料僅能揭露給位於歐盟以外的第三方 (和資料輸入者位於同一國家、或其他第三方國家，以下稱「**後續傳輸**」)，前提是該第三方同意受本條款拘束 (適用適當之模組條款)，或

(i) 該後續傳輸係傳輸至歐盟規則第 2016/679 號第 45 條之具備「適當保護程度」之國家；
(ii) 該第三方確保其依歐盟規則第 2016/679 號第 46 條或第 47 條為該資料處理提供適當之安全措施；
(iii) 該後續傳輸是於特定行政、監管、或司法程序下為建立、行使或防禦法律上之請求所必須；或
(iv) 該後續傳輸是為保護資料主體或其他自然人之重要利益所必須。

任何後續傳輸之前提是，資料輸入者須遵循本條款所有其他保護措施，特別是目的限制。

8.9 書面紀錄與條款遵循

(a) 資料輸入者應及時並適切地處理資料輸出者或資料控制者關於本條款下資料處理之詢問。
(b) 本條款當事人應能說明其對本條款之遵循情形，特別是資料輸入者應保存代表資料控制者進行資料處理活動之適當書面紀錄。
(c) 資料輸入者應向資料輸出者提供所有足以說明其對本條款之義務遵循情形之資訊，資料輸出者應將該說明提供給資料控制者。
(d) 每隔一段合理期間或當有跡象顯示有未能遵循本條款之情形發生時，資料輸入者應准許並配合資料輸出者對本條款下資料處理活動進行稽核。以上並適用於當資料輸出者基於資料控制者之指示而進行稽核之場合。於決定採取審查或稽核時，資料輸出者得考量資料輸入者是否持有相關認證。
(e) 當資料輸出者基於資料控制者之指示進行稽核時，資料輸出者應將稽核結果提供給資料控制者。
(f) 資料輸出者得選擇自行或聘請獨立稽核機關以進行稽核，稽核得包含至資料輸入者之處所或實體設施進行檢視、並應於可行時給予資料輸入者合理之事前通知。

當相關監管機關要求時，本條款當事人應提供上述(b)/(c)之資訊 (包含稽核結果)。

第 9 項

使用委外廠商 (Sub-processor)

模組 2：資料傳輸「控制者」至「處理者」

(a) **概括書面授權**：資料輸入者已取得資料輸出者之概括書面授權而得以委任列於雙方合意清單之委外廠商。若資料輸入者欲變更該清單 (增加或替換委外廠商)，應至少提前 30 天以書面通知資料輸出者，以給予資料輸出者足夠時間於資料輸入者委任委外廠商前拒絕此項變更。為使資料輸出者得以行使此項權利，資料輸入者應向其提供必要資訊。

(b) 若資料輸入者委任委外廠商 (代表資料輸出者) 進行特定之資料處理活動，資料輸入者應予委外廠商簽署書面合約，該合約中應包含與本條款相同之資料輸入者資料保護義務條款，包含資料主體得以第三方受益人身分行使權利。本條款當事人同意，若資料輸入者符合本條款要求，即表示資料輸入者盡到第 8.8 項下之義務。

(c) 資料輸入者應依資料輸出者之要求，提供一份其與委外廠商間合約 (包含後續增補協議) 之複印本。於保護商業秘密或其他機密資訊 (包含個人資料) 之必要範圍內，資料輸入者於提供複印本前得將合約文字刪減。

(d) 資料輸入者應對委外廠商就其與資料輸入者間合約義務之履行對資料輸出者負責。若委外廠商無法履行該合約義務，資料輸入者應通知資料輸出者。

(e) 資料輸入者應於其與委外廠商間合約納入第三方受益人條款- 即當資料輸入者事實上消失、法律上不再存續或已無清償能力者，資料輸出者應有權終止資料輸入者與委外廠商間之合約，且有權指示委外廠商刪除或返還個人資料。

模組 3：資料傳輸「處理者」至「處理者」

(a) **概括書面授權**：資料輸入者已取得資料控制者之概括書面授權而得以委任列於雙方合意清單之委外廠商。若資料輸入者欲變更該清單 (增加或替換委外廠商)，應至少提前 30 天以書面通知資料控制者，以給予資料控制者足夠時間於資料輸入者委任委外廠商前拒絕此項變更。為使資料控制者得以行使此項權利，資料輸入者應向其提供必要資訊。資料輸入者應將委任委外廠商之事實通知資料輸出者。

(b) 若資料輸入者委任委外廠商 (代表資料控制者) 進行特定之資料處理活動，應與委外廠商訂立書面合約，該合約中應包含與本條款相同之資料輸入者資料保護義務條款，包含資料主體得以第三方受益人身分行使權利。本條款當事人同意，若資料輸入者符合本條款要求，即表示資料輸入者盡到第 8.8 項下之義務。資料輸入者應確保委外廠商盡到資料輸入者於本條款下應負之義務。

(c) 資料輸入者應依資料輸出者或資料控制者的要求，提供一份其與委外廠商間合約 (包含後續增補協議) 之複印本。於保護商業秘密或其他機密資訊 (包含個人資料) 之必要範圍內，資料輸入者於提供複印本前得將合約文字刪減。

(d) 資料輸入者應對委外廠商就其與資料輸入者間合約義務之履行對資料輸出者負責。若委外廠商無法履行該合約義務，資料輸入者應通知資料輸出者。

(e) 資料輸入者應於其與委外廠商間合約納入第三方受益人條款- 即當資料輸入者事實上消失、法律上不再存續或已無清償能力者，資料輸出者應有權終止資料輸入者與委外廠商間之合約，且有權指示委外廠商刪除或返還個人資料。

第 10 項

資料主體權利行使

模組 2：資料傳輸「控制者」至「處理者」

(a) 資料輸入者收到資料主體之任何請求時，應及時通知資料輸出者。除非獲得資料輸出者之授權，資料輸入者不得擅自回覆該請求。

(b) 資料主體依歐盟規則第 2016/679 號行使資料主體權利時，資料輸入者應協助資料輸出者履行其回覆義務。基此，本條款當事人應於**附件 II** 列出適當的技術及組織措施，應考量資料處理的本質、應提供之協助、協助之範圍及程度。

(c) 資料輸入者須遵守資料輸出者之指示，以履行其於前述(a)/(b)之義務。

模組 3：資料傳輸「處理者」至「處理者」

(a) 資料輸入者收到資料主體之任何請求時，應及時通知資料輸出者及 (若可行) 資料控制者。除非獲得資料輸出者之授權，資料輸入者不得擅自回覆該請求。

(b) 資料主體依歐盟規則第 2016/679 號或第 2018/1725 號行使資料主體權利時，資料輸入者應協助資料輸出者或資料控制者履行其回覆義務。基此，本條款當事人應於**附件 II** 列出適當的技術及組織措施，應考量資料處理的本質、應提供之協助、協助之範圍及程度。

第 11 項

申訴

(a) 資料輸入者應以透明且方便取得之格式，透過個別通知或於其網站上揭示其處理申訴之聯絡窗口，並應及時處理其自權利主體收到之申訴。

模組 2：資料傳輸「控制者」至「處理者」

模組 3：資料傳輸「處理者」至「處理者」

(b) 若資料主體與本條款任一當事人針對其是否遵循本條款而發生紛爭，該當事人應盡商業上合理努力和平地、及時地解決紛爭。本條款當事人應使他方知悉該紛爭，並 (可行時) 合作解決紛爭。

(c) 當資料主體依本條款第 3 項行使第三方受益人權利，資料輸入者於以下情形下應接受資料主體之決定：

(i) 向資料主體居所地或工作地之歐盟成員國之相關監管機關、依本條款第 13 項規定之有管轄權之監管機關提出申訴；

(ii) 將紛爭提交給本條款第 13 項之有管轄權法院。

(d) 本條款當事人同意，非營利實體、組織或協會於歐盟規則第 2016/679 號第 80 條(1) 規定下得代表資料主體。

(e) 資料輸入者應遵從在相關歐盟或其成員國法令下有拘束力之決定。

(f) 資料輸入者同意，資料主體所為之決定不會影響其依相關法令所享有的實體上及程序上之救濟權利。

第 12 項

責任

模組 2：資料傳輸「控制者」至「處理者」

模組 3：資料傳輸「處理者」至「處理者」

(a) 本條款任一方當事人應對其違反本條款而對他方當事人所造成之損害負責。

(b) 資料輸入者或其委外廠商因違反本條款之第三方受益人權利而導致資料主體受有任何重大或非重大損害者，資料輸入者應對資料主體負責，資料主體有權向資料輸入者請求賠償。

(c) 儘管前述(b)之規定，資料輸出者、資料輸入者 (或其委外廠商) 因違反本條款之第三方受益人權利而導致資料主體受有任何重大或非重大損害者，資料輸出者應對資料主體負責，資料主體有權向資料輸入者請求賠償。本規定不影響歐盟規則第 2016/679 號及歐盟規則第 2018/1725 號規定下資料輸出者之責任、及 (當資料輸出者為資料控制者之資料處理者時) 資料控制者之責任。

(d) 本條款當事人同意，若資料輸出者依前述(c)規定因資料輸入者 (或其委外廠商)而應對資料主體負責時，資料輸出者得請求資料輸入者依責任比例分擔責任。

(e) 若本條款多數當事人均因違反本條款規定而應對資料主體負責時，該等當事人應對資料主體負共同連帶責任，而資料主體得分別向任一當事人起訴請求。

(f) 本條款當事人同意，若任一當事人依前述(e)規定須對資料主體負責時，其得請求其他當事人依責任比例分擔賠償額。

(g) 資料輸入者藉由委外廠商的行為以逃避自己的責任。

第 13 項

監管

模組 2：資料傳輸「控制者」至「處理者」

模組 3：資料傳輸「處理者」至「處理者」

(a) [**若資料輸出者係於歐盟成員國境內設立之實體：**] 列於**附件 I.C** 有義務確保資料輸出者遵循歐盟規則第 2016/679 號之資料傳輸規定之監管機關，應為有管轄權之監管機關。

[若資料輸出者雖非於歐盟成員國境內設立之實體，但符合歐盟規則第 2016/679 號第 3 條(2)之地域效力規定且已依歐盟規則第 2016/679 號第 27 條(1)規定指派一位代表

人：] 列於**附件 I.C** 而依歐盟規則第 2016/679 號第 27 條(1)規定選出之代表人所在之歐盟成員國之監管機關，應為有管轄權之監管機關。

[若資料輸出者雖非於歐盟成員國境內設立之實體，但符合歐盟規則第 2016/679 號第 3 條(2)之地域效力規定而未依歐盟規則第 2016/679 號第 27 條(1)規定指派一位代表人：] 因提供產品或服務給資料主體或資料主體之行為被監控，而將資料主體之個人資料進行跨境傳輸，該資料主體所在之歐盟成員國 (列於**附件 I.C**) 之監管機關，應為有管轄權之監管機關。

(b) 資料輸入者同意接受有管轄權監管機關之管轄，並在任何確保本條款遵循之程序中配合有管轄權監管機關。特別是，資料輸入者同意回覆監管機關之詢問、接受稽核及遵守監管機關所採行之措施，包含補救與賠償措施。資料輸入者應向監管機關提供書面確認，確認其已採行必要行動。

第 III 條—政府機關(Public Authorities)有存取權限時之相關當地法令及義務

第 14 項

影響本條款遵循之當地法令及慣例

模組 2：資料傳輸「控制者」至「處理者」

模組 3：資料傳輸「處理者」至「處理者」

(a) 本條款當事人擔保其沒有理由相信，資料輸入者處理個人資料之第三方國家之法令或慣例 (包含任何使揭露個人資料之規定、或授權政府機關存取之措施) 將阻礙資料輸入者遵守本條款規定。這是基於，尊重自然人之基本權利及自由、且不逾越民主社會下必要性及合比例性要求以保障歐盟規則第 2016/679 號第 23 條(1)規定任一目標之第三方國家法令或慣例，將不會與本條款規定衝突。

(b) 本條款當事人聲明，為達成前項擔保，其已適切地考量以下要素：

(i) 資料傳輸之具體情形，包含資料處理流程之長度、參與處理者之數量、所使用之傳輸管道、預期的後續傳輸、資料收受者之類型、資料處理之目的、所傳輸個人之料之種類及格式、資料傳輸發生於何經濟產業、資料傳輸所儲存之地點；

(ii) 資料傳輸目的地第三方國家之法令及慣例，包含要求將資料揭露給政府機關或開放存取權限給該等機關之法令及慣例 (考量資料傳輸之具體情形，及相關限制與保護措施)；

(iii) 任何相關用以補充本條款所定保護措施之合約上、技術或組織保護措施，包含資料傳輸時所應用之措施、及在資料傳輸目的地第三方國家進行資料處理所應用之措施。

(c) 資料輸入者擔保，為履行前述(b)規定，其已盡商業上合理努力向資料輸出者提供相關資訊，並同意持續與資料輸出者合作以遵循本條款規定。

(d) 本條款當事人同意紀錄前述(b)規定之評估，並當有管轄權監管機關要求時，提供給該監管機關。

(e) 若資料輸入者於接受本條款規定並於合約其間內，有理由相信其將受或已受法令或慣例拘束，而該法令或慣例與前述(a)規定不符 (包含遵循第三方國家之法令修正或措施 (例如揭露要求) 意味著適用該等法律將與前述(a)規定不符)，資料輸入者同意及時通知資料輸出者。[針對模組 3：資料輸出者應將該通知向資料控制者轉達]

(f) 資料輸出者收受前述(e)之通知、或其有理由相信資料輸入者無法繼續履行本條款之義務者，資料輸出者應及時提出適當之措施 (即得以確保資訊安全及保密之技術或組織措施)，以供資料輸出者及/或資料輸入者採行。[針對模組 3：若可行，資料輸出者應諮詢資料控制者] 若資料輸出者認為無適當之保護措施，或依 [針對模組 3：資料控制者或] 有管轄權監管機關之指示，資料輸出者應停止進行資料傳輸。於此情形下，資料輸出者在本條款資料處理之範圍內，有權終止本條款合約。若本條款合約之當事人多於二位，除非當事人另有合意，否則資料輸出者僅得終止其與有關當事人間之本條款合約，若本條款依本(f)規定終止，則適用第 16 項(d)及(e)之規定。

第 15 項

政府機關(Public Authorities)有存取權限時資料輸入者之義務

15.1 通知

(a) 若有以下情形，資料輸入者同意及時通知資料輸出者及 (若可行) 資料主體 (若有必要且在資料輸出者之協助下)：

(i) 收受政府機關依資料傳輸目的地第三方國家關於揭露經傳輸之個人資料而有法律效力之請求 (該政府機關包含司法機關)；此項通知應包含該政府機關所請求之個人資料、該政府機關之資訊、該請求所依據之法律基礎、資料輸入者所提供之回覆；或

(ii) 知悉經傳輸之個人資料被資料傳輸目的地第三方國家之政府機關依當地法令直接存取；此項通知應包含所有資料輸入者所可得之資訊。

[針對模組 3：資料輸出者應將該通知向資料控制者轉達。]

(b) 若依資料傳輸目的地第三方國家規定，資料輸入者不得通知資料輸出者及/或資料主體，資料輸入者同意盡其商業上合理努力、盡快、盡可能提供資訊，以取得該禁止規定之豁免權。資料輸入者同意紀錄其努力之作為，以於資料輸出者要求時，向資料輸出者說明。

(c) 在資料傳輸目的地第三方國家允許之前提下，資料輸入者同意於本條款合約期間內定期向資料輸出者盡可能提供關於政府機關請求之資訊，特別是請求之數量、所請求之資料之類型、請求之機關、資料輸入者是否對該請求提出質疑、提出質疑後之結果等。[針對模組 3：資料輸出者應將該通知向資料控制者轉達。]

(d) 資料輸入者同意於本條款合約期間內保存前述(a)至(c)之資料，並於有管轄權監管機關要求時，將資料提供給該監管機關。

(e) 前述(a)至(c)規定不影響本條款第 14 條(e)及第 16 條關於資料輸入者應及時通知資料輸出者之規定。

15.2 合法性及資料最小化之審查

(a) 資料輸入者同意審查揭露個人資料之請求之合法性 (特別是該請求是否在該提出請求之政府機關之權限範圍內)，並經審慎評估後認為有合理理由決定該請求在資料傳輸目的地第三方國家法令、國際法及國際禮讓原則下為不合法，資料輸入者同意對該請求提出質疑。在相同條件下，資料輸入者應在可能之情況下提出上訴。於提出質疑時，資料輸入者應尋求暫時處置措施以使該請求之效力暫時停止，直至有管轄權司法機關作出實質裁決。資料輸入者僅能在相關程序法令之要求下揭露個人資料。以上規定不影響本條款第 14 條(e)規定下資料輸入者之義務。

(b) 資料輸入者同意記錄其法律上之評估及對揭露請求所提出之質疑，並在資料傳輸目的地第三方國家法令允許之範圍內，將該等紀錄提供給資料輸出者，並應依有管轄權監

管機關之請求，將該等紀錄提供給該監管機關。[針對模組 3：資料輸出者應將該評估提供給資料控制者。]

(c) 資料輸入者同意，於回應揭露請求時，在合理解讀該請求之情況下，僅提供最小數量之資料給請求機關。

第 IV 條—最終條款

第 16 項

本條款之違反、終止規定

(a) 若資料輸入者出於任何原因無法遵守本條款規定，應及時通知資料輸出者。

(b) 若資料輸入者違反或無法遵守本條款規定，資料輸出者應暫停將資料傳輸給資料輸入者，直至資料輸入者遵守本條款規定或本條款合約被終止。本款規定不影響第 14 條(f)規定。

(c) 有以下情形者，資料輸出者在本條款資料處理之範圍內，有權終止本條款合約：

(i) 資料輸出者已依前述(b)規定暫停將資料傳輸給資料輸入者，且於合理期間內 (最長不超過暫停傳輸後之一個月內) 資料輸入者仍不能遵守本條款規定；

(ii) 資料輸入者重大或持續違反本條款規定；

(iii) 資料輸入者未能遵循有管轄權法院或監管機關對於資料輸入者於本條款下義務所作之有拘束力決定。

(d) 有上述情形者，資料輸出者應將此等未遵循本條款之情形告知有管轄權監管機關 [針對模組 3：及資料控制者] 。若本條款合約之當事人多於二位，除非當事人另有約定，否則資料輸出者僅得終止與有關當事人間之合約。

(e) 於本條款合約終止前已依前述(c)規定傳輸之個人資料，資料輸入者應及時將該資料刪除，包含該資料之複印本。資料輸入者應項資料輸出者確認資料已刪除。在資料刪除前，資料輸入者應繼續遵守本條款規定。若資料輸入者所在當地法令禁止資料輸入者將資料刪除，則資料輸入者應擔保其會持續遵循本條款規定並僅於當地法令允許之範圍內處理個人資料。

(f) 有以下情形者，本條款任一方當事人得撤回其受本條款拘束之意思表示：(i) 歐盟委員會依歐盟規則第 2016/679 號第 45 條(3)關於個人資料傳輸之規定所採行之決定，而本條款適用該決定；(ii) 歐盟規則第 2016/679 號已成為資料傳輸目的地國家之法令體

系之一部分。本款規定不影響相關資料傳輸於歐盟規則第 2016/679 號下應負之義務。

第 17 項

準據法

模組 2：資料傳輸「控制者」至「處理者」

模組 3：資料傳輸「處理者」至「處理者」

本條款之準據法為英國法。若該法律不允許第三方受益人權利，則本條款應受其他准許第三方受益人權利之歐盟成員國法律拘束，而該歐盟成員國法律為愛爾蘭。

第 18 項

合意管轄條款

模組 2：資料傳輸「控制者」至「處理者」

模組 3：資料傳輸「處理者」至「處理者」

(a) 任何因本條款引起之爭議，本條款當事人同意由倫敦法院管轄。

(b) 資料主體得向其居住地之歐盟成員國法院對資料輸出者及/或資料輸入者提出法律程序。

(c) 本條款當事人同意受以上法院之管轄。

附件

附件 I

A. 當事人名單

模組 2：資料傳輸「控制者」至「處理者」

模組 3：資料傳輸「處理者」至「處理者」

資料輸出者：

1. 姓名/名稱：
   您 (DeepQ AI Platform 之使用者)
2. 地址或電子郵件：
   如同您提供給 DeepQ 之聯繫方式
3. 聯絡人之姓名/職位/聯繫資訊：
   如同您提供給 DeepQ 之聯繫方式
4. 於本條款下針對所傳輸之個人資料所進行之活動：
   基於 AI 模型訓練及部署之目的，將可能含有個人資料之影像上傳至 DeepQ AI Platform 或提供給 DeepQ。
5. 角色：
   資料控制者或資料處理者 (依具體情形決定) 。

資料輸入者：

1. 名稱：
   奧啓迪科技股份有限公司
2. 地址：
   231 台灣新北市新店區北新路三段 207-5 號 13 樓
3. 聯絡人之姓名/職位/聯繫資訊：
   資料保護官，global-privacy@htc.com
4. 於本條款下針對所傳輸之個人資料所進行之活動：

DeepQ 僅會在您的指示下處理您上傳至 DeepQ AI Platform 或提供給 DeepQ 而可能含有個人資料之影像；該資料處理活動可能包含影像上傳測試、刪除影像、變更影像之檔案格式、及其他形式之處理。

5. 角色：
   資料處理者。

B. 資料傳輸之描述

模組 2：資料傳輸「控制者」至「處理者」

模組 3：資料傳輸「處理者」至「處理者」

被傳輸之個人資料所屬之資料主體類別：如資料輸出者上傳或提供之影像所示。

被傳輸之個人資料類別：如資料輸出者上傳或提供之影像所示。

被傳輸之敏感性個人資料 (如有適用) 及所適用之限制或安全措施：僅有經授權、且有存取需要之人員及第三方服務提供者得存取個人資料。

個人資料傳輸之頻率：一次性傳輸。

個人資料處理之本質：資料代管與資料庫服務。

個人資料傳輸與後續傳輸之目的：將個人資料傳輸給指定之第三方服務提供者以提供資料代管與資料庫服務。

個人資料留存期間或 (若無法訂定留存期間) 用以決定個人資料留存期間之標準：個人資料將於資料輸出者 (i) 保有 DeepQ AI Platform 授權使用者身分之期間內，及 (ii) 此授權使用期間屆至或終止後一年內 (基於 DeepQ 繼續進行適當管理及行政目的) 留存。

個人資料傳輸給委外廠商時，個人資料處理的主要內容、本質及期間：基於資料代管與資料庫服務之目的，個人資料將會傳輸給指定之第三方服務提供者。個人資料將於資料輸出者 (i) 保有 DeepQ AI Platform 授權使用者身分之期間內，及 (ii) 此授權使用期間屆至或終止後一年內 (基於 DeepQ 繼續進行適當管理及行政目的) 留存

C. 有管轄權之監管機關

模組 2：資料傳輸「控制者」至「處理者」

模組 3：資料傳輸「處理者」至「處理者」

[若資料輸出者係於歐盟成員國境內設立之實體：] 資料輸出者設立國家之監管機關。

[若資料輸出者雖非於歐盟成員國境內設立之實體，但符合歐盟規則第 2016/679 號第 3 條(2)之地域效力規定且已依歐盟規則第 2016/679 號第 27 條(1)規定指派一位代表人：] 資料輸出者代表人設置國家之監管機關。

[若資料輸出者雖非於歐盟成員國境內設立之實體，但符合歐盟規則第 2016/679 號第 3 條(2)之地域效力規定而未依歐盟規則第 2016/679 號第 27 條(1)規定指派一位代表人：] 資料主體所在任一歐盟成員國之監管機關。

附件 II—技術及組織措施 (包含確保資訊安全之技術及組織措施)

模組 2：資料傳輸「控制者」至「處理者」

模組 3：資料傳輸「處理者」至「處理者」

- 個人資料匿名化及加密之措施：
  已遵循 DeepQ Security 文件 S-G20-03 Information Asset Category and Group, S-O21Encrpytion Management Process
- 確保個人資料處理系統及服務持續具有保密性、完整性、可用性及靈活性之措施：
  已遵循 DeepQ Security 文件 S-O19-01, Disaster Recovery Plan, S-O19-02 Disaster Recovery Drill Report
- 當發生實體或技術資料安全事件時，確保及時回復對個人資料之可得性及存取權限之措施：
  已遵循 DeepQ Security 文件 S-O19-01, Disaster Recovery Plan, S-O19-02 Disaster Recovery Drill Report
- 為確保個人資料處理之安全性，定期測試、存取及評估技術及組織措施之有效性之程序：
  已遵循 DeepQ Security 文件 S-G18 Information System Acquisition Development and Maintenance Guidelines
- 辨識使用者身分及授權機制之措施：
  已遵循 DeepQ Security 文件 S-O06 Account Management Process
- 個人資料傳輸之保護措施：
  已遵循 DeepQ Security 文件 S-G20-03 Information Asset Category and Group, S-O21Encrpytion Management Process
- 個人資料儲存之保護措施：
  已遵循 DeepQ Security 文件 S-G20-03 Information Asset Category and Group, S-O21Encrpytion Management Process
- 確保個人資料處理場域之實體安全之措施：
  已遵循 DeepQ Security 文件 S-O02 Physical Security Process
- 確保資安事件紀錄之措施：
  已遵循 DeepQ Security 文件 S-O12 Log Management Process
- 確保系統設定 (包含預設設定)：

已遵循 DeepQ Security 文件 S-G18 Information System Acquisition Development and Maintenance Guidelines

- 內部資訊科技及資訊科技安全監督及管理措施：
  已遵循 DeepQ Security 文件 S-O07 System Operation Process, S-O04 Network Security Management Process
- 流程及產品之認證及保證措施：
  已遵循 DeepQ Security 文件 S-O16 Application Development and Deployment Security Process
- 確保個人資料最小化之措施：
  已遵循 DeepQ Security 文件 P-G06 Personal Information Processing Guideline
- 確保個人資料品質之措施：
  已遵循 DeepQ Security 文件 P-G06 Personal Information Processing Guideline
- 確保有限度之個人資料留存期限之措施：
  已遵循 DeepQ Security 文件 P-G06 Personal Information Processing Guideline
- 確保可歸責性之措施：
  已遵循 DeepQ Security 文件 S-G20 Information Asset Management Guideline, S-G02 Security Operation Guidelines

針對將個人資料傳輸給委外廠商，委任廠商所採取之技術及組織措施，以向資料控制者及資料輸出者 (當資料是由資料處理者傳輸至委外廠商) 提供協助：

2. Google: https://cloud.google.com/security

附件 III—委外廠商清單

模組 2：資料傳輸「控制者」至「處理者」

模組 3：資料傳輸「處理者」至「處理者」

您 (作為資料控制者) 同意授權下列委外廠商進行資料處理：

1. 名稱：Google (即 Google Asia Pacific Pte. Ltd., 位於新加坡)

地址：8 Marina Boulevard, #05-02, Marina Bay Financial Centre, Singapore 018981.

連絡電話：+65-65218000

資料處理之描述：Google 提供雲端運算服務 Google Cloud Platform，DeepQ AI Platform 建置於 Google Cloud Platform 上。Google 並提供 Google cloud SQL 資料庫代管服務。

附錄 III

商業夥伴協議 (Business Associate Agreement)

定義

概括定義：

本商業夥伴協議之以下用語應與「健康保險可攜與責任法」（Health Insurance Portability and Accountability Act，以下稱 HIPAA）中之 用語之意義相同：違反 (Breach)、資料聚合 (Data Aggregation)、指定紀錄組 (Designated Record Set)、揭露 (Disclosure)、 健康照顧活動 (Health Care Operations) 、個人 (Individual) 、最小必要原則 (Minimum Necessary) 、隱私作業通知 (Notice of Privacy Practices)、受保護健康資訊 (Protected Health Information)、依法律規定 (Required By Law)、秘書長 (Secretary)、資訊安全事件 (Security Incident)、分包商 (Subcontractor)、不安全之受保護健康資訊 (Unsecured Protected Health Information)、及使用 (Use).

個別定義：

(a) 商業夥伴.「商業夥伴」原則上與 45 CFR 160.103 所指之商業夥伴有相同意義，而在本協議中，商業夥伴指**奧啓迪科技股份有限公司**。
(b) 適用機構.「適用機構」原則上與 45 CFR 160.103 所指之適用機構有相同意義，而在本協議中，適用機構指**您** (即 **DeepQ AI Platform 之使用者**)。
(c) HIPAA 規定.「HIPAA 規定」指 45 CFR Part 160 及 Part 164 之隱私 (Privacy)、資訊安全 (Security)、違反規定之通知 (Breach Notification) 及執行規定。

商業夥伴之義務與活動

商業夥伴同意：

(a) 除非本協議或法律規定或允許，否則商業夥伴不會使用或揭露受保護健康資訊；
(b) 商業夥伴會使用適當的保護措施，並遵循 Subpart C of 45 CFR Part 164 關於電子形式受保護健康資訊之規定，避免以本協議未允許之方式使用或揭露受保護健康資訊；
(c) 若商業夥伴知悉有非於本協議下所提供之受保護健康資訊被使用或揭露，包含 45 CFR 164.410 所訂之不安全之受保護健康資訊外洩，及任何其所知悉的資訊安全事件；

(d) 依據 45 CFR 164.502(e)(1)(ii)及 164.308(b)(2) (若適用)，商業夥伴應確保任何代表商業夥伴創建、收受、維護或傳輸受保護健康資訊之分包商，同意受該等適用於商業夥伴之限制、條件及規定之拘束；

(e) 商業夥伴應將指定紀錄組形式之受保護健康資訊提供給適用機構，以於必要範圍內滿足適用機構於 45 CFR 164.524 下之義務；

(f) 商業夥伴應依適用機構基於 45 CFR 164.526 所下之指示或所給之同意，對指定紀錄組形式之受保護健康資訊進行修改，或採取其他措施以於必要範圍內滿足適用機構於 45 CFR 164.526 下之義務；

(g) 商業夥伴應維護並提供必要資訊，使適用組織得於必要範圍內滿足 45 CFR 164.528 下提供與揭露有關之書面紀錄之義務；

(h) 在商業夥伴履行適用機構於 Subpart E of 45 CFR Part 164 之一項或多項義務時，商業夥伴應遵守適用於適用機構之 Subpart E 規定；

(i) 商業夥伴應將其內部作業、帳簿及紀錄提供給秘書長，以使秘書長決定其使否遵循 HIPAA 規定。

商業夥伴被允許之使用及揭露

(a) 商業夥伴僅得為履行本協議或使用條款所示之服務而使用或揭露受保護健康資訊。為履行本協議或使用條款所示之服務，商業夥伴被授權得依 45 CFR 164.514(a)-(c) 使用受保護健康資訊以進行去識別化。

(b) 商業夥伴僅得依法律規定使用或揭露受保護健康資訊。

(c) 商業夥伴同意依照適用組織之最小必要原則及程序而使用或揭露受保護健康資訊。

(d) 除非為以下所列的特定使用或揭露，否則商業夥伴不得以違反 Subpart E of 45 CFR Part 164 之方式使用或揭露受保護健康資訊。

(e) 商業夥伴得基於其適當管理及行政之目的、或為履行其法律義務，而使用受保護健康資訊。

(f) 商業夥伴得於以下情況下，基於其適當管理及行政之目的或為履行其法律義務，而揭露受保護健康資訊：(i) 依法律規定；(ii) 商業夥伴自受保護健康資訊接收方獲得確保，確保該資訊將被保密且僅於法律允許時或商業夥伴項其揭漏之目的範圍內使用或進一步揭露，且若接收方知悉該保密措施被違反時，將通知商業夥伴。

(g) 商業夥伴得提供關於適用組織健康照顧活動之資料聚合服務。

適用機構向商業夥伴通知隱私作業及限制之規定

(a) 若適用機構應將其於 45 CFR 164.520 下之隱私作業通知之限制，於該限制可能影響商業夥伴對受保護健康資訊之使用或揭露之範圍內，向商業夥伴告知。
(b) 若個人更改或撤回其對使用或揭露他/她的受保護健康資訊之同意，於該改變可能影響商業夥伴對受保護健康資訊之使用或揭露之範圍內，適用機構應向商業夥伴告知。
(c) 若適用機構同意或依 45 CFR 164.52 規定就受保護健康資訊之使用或揭露受有限制，於該限制可能影響商業夥伴對受保護健康資訊之使用或揭露之範圍內，適用機構應向商業夥伴告知。

適用機構受許可之請求

除非本協議另有規定，適用機構不應要求商業夥伴以違反 Subpart E of 45 CFR Part 164 之方式使用或揭露受保護健康資訊。

協議期間與終止

(a) 協議期間. 本協議之有效期間自適用機構與商業夥伴間之使用條款生效日起，至使用條款失效日或適用機構依後述(b)規定終止本協議之日 (以先發生者為準) 止。
(b) 違約終止. 若適用機構認為商業夥伴違反本協議任一重要條款且未於收到適用機構違約通知後之 2 個月內改正或中止違約情形，商業夥伴同意適用機構得終止本協議。
(c) 協議終止後商業夥伴之義務. 除非本協議另有規定，本協議因任何原因終止後一年，商業夥伴應銷毀自適用機構收到之受保護健康資訊、或代表適用機構創建、維護或接收而仍由商業夥伴保存之受保護健康資訊。商業夥伴不得保留任何受保護健康資訊之副本。

    若有適用，針對自適用機構收到之受保護健康資訊、或代表適用機構創建、維護或接收之受保護健康資訊，商業夥伴應：

    (i) 為其適當管理及行政之目的或為履行其法律義務之必要範圍內，留存必要之受保護健康資訊；

(ii) 將商業夥伴仍以任何形式留存之剩餘受保護健康資訊返還 (或經適用機構同意而銷毀) ；

(iii) 繼續使用適當的保護措施並遵循 Subpart C of 45 CFR Part 164 關於電子形式受保護健康資訊之規定，以避免商業夥伴在保存受保護健康資訊期間內使用或揭露該等資訊 (除非本條另有規定)；

(iv) 除於本協議終止前基於上述「商業夥伴被允許之使用及揭露」第(e)/(f)款規定所留存之受保護健康資訊，商業夥伴不得使用或揭露其留存之受保護健康資訊；及

(v) 當商業夥伴不再因適當管理及行政之目的或履行其法律義務而需要留存受保護健康資訊時，商業夥伴應將受保護健康資訊返還給適用機構 (或經適用機構同意而銷毀)。

(d) 存續條款. 商業夥伴於本條規定下之義務於本協議終止後繼續存續。

一般事項

(a) 法規索引. 本協議中提及之 HIPAA 規定，指的是有效或修正後之規定。

(b) 本協議之修改. 本協議當事人同意，為遵循 HIPAA 規定或其他法令規定，而於必要時修正本協議規定。

(c) 文義解釋. 本協議有任何不清楚之處，應依 HIPAA 規定解釋。