Diagnocat

DATA PROCESSING ADDENDUM

Date of last update – November 2026

This Data Processing Addendum ("**Addendum**") forms an integral part of the TERMS & CONDITIONS DGNCT LLC ("**Terms**"). In the case of any conflict between this Addendum and/or the Terms, the Addendum shall control.

The defined terms in the Terms shall have the same meaning in this Addendum unless otherwise specified herein. In case of questions about this Addendum, please contact privacy@diagnocat.com

1. **Data Processing**

1.1. **Definitions**. In this Addendum, the following terms will have the following meanings:

(a) "**Account**" means an account on the Site assigned to the Customer, which is used by the latter to store and manage Patient Data.

(b) "**Data Protection Law**" means applicable data protection or privacy laws or regulations in the country in which the Customer practices dentistry with respect to Customers, including (i) the Brazilian General Data Protection Law effective on 18 September 2020, (ii) the Privacy and Electronic Communications Directive (2002/58/EC), (iii) the GDPR being, as applicable, Regulation 2016/679 of the European Parliament and of the Council 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) (the "EU GDPR"), or the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR") (iv) the Switzerland ("Swiss") Federal Act on Data Protection(each as amended), (v) US HIPAA and regulations made thereunder, including the Standards for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Parts 160 and 164; the security and privacy provisions of the American Recovery and Reinvestment Act of 2009; (vi) Australia's Privacy Act 1988 (Cth), including the Australian Privacy Principles; (vii) China's Cybersecurity Law of 2017; Personal Information Protection Law of 2021; (viii) Hong Kong's Personal Data (Privacy) Ordinance (Chapter 486 of Laws of Hong Kong) ("PDPO"); (ix) Japan's Act on the Protection of Personal Information ("APPI"); (x) New Zealand's Privacy Act 2020 (NZ) including the Information Privacy Principles; (xi) Russian Federation's Federal Law No. 152-FZ on Personal Data; (xii) Singapore's Personal Data Protection Act of 2012; (xiii) South Korea's Personal Information Protection Act; (xiv) Taiwan's Personal Data Protection Act ("PDPA"); (xv) Vietnam's Civil Code, Cyber-Information Security Law and personal data protection legislations, (xvi) Thailand's Personal Data Protection Act each as they may be amended, superseded, or replaced, as well as any other applicable data protection laws or regulations.

(c) "**Data Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

(d) "**Personal Data**", "**Sensitive Personal Data**" (which shall be read as "**special categories of data**" where local Data Protection Law instead uses such term), "**process/processing**", "**Controller**" (which shall be read in this Addendum as

"Operator" where local Data Protection Law uses instead the term "Operator"), "**Processor**", will each have the meaning given to them under Data Protection Law;

(e) "**Patient**" means an individual to whom Customer provides medical services.

(f) "**Patient Data**" means the Personal Data (including confidential personal data) of the Customer's patient and "Protected Medical Information" as defined by HIPAA, including x-ray images, patient records, intraoral scans, research models and treatment plans.

(g) "**Parties**" means Diagnocat and Customer.

(h) "**SaaS**" means Diagnocat SaaS available online (via the Site) to the Customer and used by the latter in identifying anatomical areas, general conditions, and previous treatments during initial dental consultations, follow-up patients, control X-rays, and other situations that require examination and interpretation of digital images.

(i) "**Site**" means www.diagnocat.com web site.

1.2. **Responsibilities of the Parties**: Customer is the Controller of any Patient Data processed in SaaS and shall comply with Data Protection Law with respect to Patient Data. Where the Customer is a healthcare professional working with a certain legal entity - medical organization/clinic, the Controller of Patient Data will be the legal entity that determines the purposes for which, and the means by which, Patient Data is processed. To the extent that Diagnocat processes any such Patient Data, Diagnocat will do so as a Processor on Customer's behalf and in accordance with Customer's documented instructions and this Addendum.

1.3. **Responsibilities of the Customer**: Customer must inform Customer's Patients that Customer is the Controller of the Patient Data and provide Customer's contact details (including details of the Customer's data protection officer where applicable), about the purpose for which the Patient Data is being collected, the legal basis for such processing, the intended recipients of the Patient Data, name and address of the person collecting and storing Patient Data (including Diagnocat and any Subprocessors as defined below), that Patient Data may be processed in non-EU countries by Diagnocat in accordance with this Addendum, of any other information that Customer's Patients must be informed of at the time Patient Data is obtained Customer confirms that it has a lawful basis under applicable Data Protection Law for the processing of Patient Data under this Addendum, including, where the EU GDPR, the UK GDPR or the FADP applies, a condition for processing health data under Article 9 GDPR (such as Article 9(2)(h) GDPR) or the equivalent provision of local law. Where consent is the applicable legal basis, or is otherwise required by the locally applicable Data Protection Law (for example, for cross-border transfers), Customer shall obtain such consent from its Patients in the format that law requires. Customer agrees to indemnify and hold harmless Diagnocat and its directors, employees, agents, subcontractors, and affiliates from and against any claims, damages, liabilities, expenses or penalties Diagnocat may incur to the extent arising from Customer's failure to have a lawful basis for, or to provide any notice or obtain any consent required for, the disclosure of Patient Data to Diagnocat, or any of their agents, subcontractors or affiliates pursuant to this Addendum. This indemnity does not limit any right of a data subject or consumer that cannot be restricted under applicable law.

1.4. **Patient Data processing in SaaS and disclosures**. Customer will only process in SaaS and disclose to Diagnocat and third party healthcare professionals via SaaS Patient Data that is necessary to perform the Customer's obligations with respect to the relevant Patients of Customer. Where consent is the applicable legal basis or is otherwise required by the locally applicable Data Protection Law, Customer shall ensure that

Patients sign a Patient Consent form (a template form may be provided to Customer upon its request). Customer shall maintain a copy of this Patient Consent form for their records.

1.5. **Confidentiality**. Both Customer and Diagnocat agree to adhere to the principles of medical confidentiality in relation to Patient Data. Diagnocat shall ensure that any person it authorizes to process Patient Data has committed themselves to keep such Patient Data confidential (save where such person is already subject to a statutory duty of confidentiality that applies to such processing).

1.6. **Security**. Customer must use the security features (including any password, key, PIN, token or smartcard) that Diagnocat issues to Customer to access the Account individually to keep Patient Data secure and keep such security features confidential without lending, sharing, transferring or otherwise misusing them. Customer acknowledges that Diagnocat may change its security features from time to time. Diagnocat shall implement appropriate technical and organisational measures against unauthorised or unlawful processing of Patient Data and against accidental loss or destruction of or damage to Patient Data taking into account the harm that might result from such unauthorised or unlawful processing, loss, destruction or damage and the nature of the Patient Data to be protected. Diagnocat's security measures, including encryption and related controls, comply with ISO 27001 requirements and are certified under ISO/IEC 27001. These measures include, at a minimum: (a) role-based access with least privilege, single sign-on and multi-factor authentication, access to production only through a VPN or jump host, annual access reviews and revocation of leavers' access within 24 hours; (b) encryption of Patient Data transmitted over public or untrusted networks using secure protocols such as TLS, and encryption of Patient Data stored in systems controlled by Diagnocat using appropriate industry-standard encryption mechanisms and secure key management practices; (c) logical separation of each Customer's data, network segmentation, separation of development from production, and web application firewall and DDoS protection; (d) an OWASP-based security review of every release, quarterly vulnerability scans and an annual external penetration test, with critical vulnerabilities remediated within 72 hours; (e) daily backups, multi-zone hosting and annual disaster recovery and business continuity tests; (f) non-disclosure agreements, background checks and security and privacy training for personnel; and (g) an annual information security risk assessment, a dedicated incident response function, and risk assessment of suppliers before engagement and periodically thereafter. Diagnocat may update its security measures from time to time, provided that the overall level of protection of Patient Data is not reduced.

1.7. **Subprocessing**. Customer authorizes Diagnocat to engage third parties, including affiliated entities of Diagnocat, to process Patient Data on its behalf ("**Subprocessors**"). Diagnocat maintains an up-to-date list of its Subprocessors, the services they provide and their locations, which it will make available to Customer on request at privacy@diagnocat.com. As of the effective date of this Addendum, Patient Data is hosted and processed on Google Cloud Platform (Google LLC). Diagnocat will give Customer at least thirty (30) days' prior notice of any intended addition or replacement of a Subprocessor. Customer may object in writing on reasonable data protection grounds within fifteen (15) days after receiving such notice. The Parties will work in good faith to resolve the objection; if they cannot, Diagnocat may, at its option, make a commercially reasonable change to the SaaS to avoid the affected processing or allow Customer to terminate the affected services without penalty. Diagnocat will impose on each

Subprocessor, by written agreement, data protection obligations no less protective than those in this Addendum, and remains responsible to Customer for the performance of its Subprocessors, subject to the liability provisions of the Terms.

1.8. **Data transfers**: Customer acknowledges that Diagnocat may transfer Patient Data for processing to one or more of its affiliates or third party Subprocessors in the course of providing the Services, which include countries outside the European Economic Area ("**EEA**"). Customer further acknowledges that Diagnocat may transfer/provide access in SaaS to the Patient Data the Customer to a third party healthcare professional in accordance with the Customer's instructions made using SaaS or otherwise. Diagnocat shall comply with the Customer's instructions in relation to transfers of Personal Data to a country outside of the EEA unless Diagnocat is required pursuant to Data Protection Law to transfer Personal Data outside the EEA, in which case Diagnocat shall inform the Customer in writing of the relevant legal requirement before any such transfer occurs, unless the Data Protection Law prohibits such notification on important grounds of public interest. Customer agrees to indemnify and hold harmless Diagnocat and its directors, employees, agents, subcontractors, and affiliates from and against any claims, damages, liabilities, expenses or penalties Diagnocat may incur due to performing the Customer's instructions to transfer/provide access in SaaS to the Patient Data to a third party healthcare professional specified by the Customer.

1.9. **Data retention**: Customer, as Controller, determines the retention period for Patient Data in accordance with applicable law and its own record-keeping obligations. Diagnocat will store Patient Data in Customer's Account for the term of the Terms, unless Customer deletes it earlier, and thereafter only for the deletion period set out in Section 1.10. Customer will be able to access and to download copies of Customer's Patients' Patient Data from Customer's Account at any time, unless and until such Patient Data is no longer retained pursuant to this Section 1.9. or Customer's authority as Controller of that Patients' Patient Data has ended pursuant to Section 1.10. Customer must comply with its own archiving and record keeping requirements and should regularly make copies of Patient Data stored in its Account for such purposes.

1.10. **Data deletion.** Diagnocat retains Patient Data in the Customer's Account in accordance with Section 1.9 unless the Customer, acting as Controller, requests deletion or the Patient Data is deleted following termination of the Services. Following such deletion request or termination, Patient Data will be removed from Diagnocat's operational systems and overwritten from back-ups within ninety (90) days, subject to the Controller's instructions and applicable law. This 90-day period reflects the standard technical window for secure deletion and does not constitute a shorter retention period under Section 1.9. Before deletion, Customer may download a copy of its Patient Data from its Account; at Customer's request, Diagnocat will confirm deletion in writing. Diagnocat may retain Patient Data after deletion only to the extent required by law applicable to Diagnocat (for example, records required for medical device vigilance and post-market surveillance), and only for the period so required; such data remains protected under this Addendum.

1.11. **Data Subject Rights:** If (a) a Patient wishes to exercise any of their data subject rights under applicable Data Protection Law in relation to their Patient Data (including its rights of access, correction, objection, erasure and data portability, as applicable); or
(b) any other correspondence is received from a data subject, data protection authority or other third party in connection with Diagnocat's processing of Patient Data, Diagnocat will promptly inform Customer of such request and provide Customer with such reasonable

assistance as Customer may require in connection with such request. Diagnocat will not respond directly to such a request, other than to refer the Patient or other requester to Customer, unless Customer instructs it in writing to do so or applicable law requires it.

1.12. **Individuals' rights**: **Anonymized data**. Customer agrees that Diagnocat may use Patient Data for promotional, educational and/ or research and development purposes, publication in professional journals or use in professional collateral materials, provided that such Patient Data has first been anonymized in a way that neither Customer nor any Patient are identifiable under applicable laws.

1.13. **Customer Personal Data**. Diagnocat acts as an independent Controller, and not as Customer's Processor, for the personal data of Customer and its authorized users, such as name, contact details, account, login and billing data ("**Customer Personal Data**"). Diagnocat processes Customer Personal Data to provide and administer the Account and the SaaS, handle orders and billing, provide support and training, and meet its own legal obligations, in accordance with applicable Data Protection Law and Diagnocat's Privacy Policy available on the Site. The Privacy Policy describes the legal bases, any marketing communications and how to opt out of them, recipients, international transfers and the data subject rights available..

1.14. **Data Breaches**. Diagnocat will notify Customer without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a Data Security Breach affecting Patient Data. The notice will describe, as far as then known: (a) the nature of the Data Security Breach; (b) the categories and approximate number of data subjects and records concerned, and the jurisdictions involved; (c) the likely consequences; (d) the measures taken or proposed to address it and mitigate its possible adverse effects; and (e) a contact point for more information. Diagnocat will provide updates as further information becomes available, will take all reasonable steps to contain, mitigate and remediate the Data Security Breach, and will assist Customer in meeting its own notification obligations to supervisory authorities and data subjects (for example, notification of the competent supervisory authority within 72 hours under the EU GDPR or UK GDPR). Diagnocat will not notify supervisory authorities or data subjects of a Data Security Breach affecting Patient Data without Customer's prior consent, unless required to do so by applicable law.

1.15. **Data hosting**. Patient Data is hosted and processed on Google Cloud Platform in the region that corresponds to Customer's location: the European Union, the United States, Canada or Australia. Patient Data of Customers located in the UK and Switzerland is hosted in the European Union region. Where local Data Protection Law requires Patient Data to be stored in a particular country, the Additional Terms for that country apply. Any transfer of Patient Data outside the hosting region will be made only in accordance with Section 1.8, the applicable Additional Terms and Data Protection Law.

1.16. **Requests from public authorities**. If Diagnocat receives a legally binding request from a public authority (including a law enforcement authority) for disclosure of or access to Patient Data, Diagnocat will, unless prohibited by law, promptly notify Customer and redirect the authority to Customer where possible. Diagnocat will review the legality of the request, challenge it where there are reasonable grounds to consider it unlawful, disclose only the minimum Patient Data required to comply with it, and document the request and its response.

1.17. **Records of processing**. Diagnocat will maintain a record of the categories of processing activities it carries out on behalf of Customer, as required by applicable Data Protection

Law (including Article 30(2) of the EU GDPR and UK GDPR and Article 12 of the FADP), and will make it available to Customer or the competent supervisory authority on request.

1.18. **Data protection impact assessments and prior consultation**. Taking into account the nature of the processing and the information available to it, Diagnocat will provide Customer with reasonable assistance in carrying out any data protection impact assessment or privacy impact assessment, and any prior consultation with a supervisory authority, that Customer is required to carry out under applicable Data Protection Law in relation to the processing of Patient Data.

2. **Additional Terms applicable to European Economic Area, the UK and Switzerland:**
In addition to the terms and conditions in Section 1 above, the following data protection terms and conditions shall apply to Customers located in markets within the European Economic Area, the UK and Switzerland.

2.1. **Subprocessing.** Customer agrees that Diagnocat may subcontract its processing of Patient Data to Subprocessors (as defined in Section 1.7. hereof) provided that: (i) Diagnocat has in place a written agreement with the Subprocessor that requires it to process Patient Data only in accordance with this Addendum; (ii) Diagnocat remains liable to Customer for ensuring that our Subprocessors process Patient Data in accordance with this Addendum. The notice and objection procedure in Section 1.7 applies to any addition or replacement of a Subprocessor.

2.2. **Data transfers**. Diagnocat shall only transfer Patient Data outside the EEA, Switzerland or the UK where it has taken such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Law. Diagnocat currently relies on Adequacy Decisions, and in the absence of such, on other appropriate transfer mechanism such as the EU Commission Standard Contractual Clauses.

2.3. **Audit**. Diagnocat shall make available to the Customer all information necessary to demonstrate compliance with the obligations set out in this Addendum and allow for and contribute to audits, including inspections, conducted by or on behalf of the Customer or by the data protection authority.

2.4. **Data protection impact assessment**. If Diagnocat believes or becomes aware that its processing of Patient Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, Diagnocat shall inform Customer and provide Customer with reasonable cooperation in connection with any data protection impact assessment and any prior consultation with the competent supervisory authority that may be required under applicable Data Protection Law, in accordance with Section 1.18.

2.5. **Data hosting and storage locations.** Patient Data of Customers located in the EEA, the UK and Switzerland is hosted in Google Cloud data centres located within the European Union, in accordance with Section 1.15. Any transfers of Patient Data outside the EEA, Switzerland, or the UK shall be made only in accordance with Section 2.2 and applicable Data Protection Law. Diagnocat may appoint new Subprocessors only in accordance with Sections 1.7 and 2.1, including the Customer's right to object on reasonable data protection grounds.

2.6. **Swiss professional secrecy.** Where Customer is bound by professional secrecy under Article 321 of the Swiss Criminal Code, Diagnocat acts as its auxiliary person and keeps Patient Data secret on the same terms.

3. **Additional Terms applicable to Israel:**

In addition to the terms and conditions in Section 1 above, the following data protection terms and conditions shall apply to Customers located in Israel.

3.1. **Subprocessing**: Customer agrees that Diagnocat may subcontract its processing of Patient Data to third parties ("Subprocessors") provided that: (i) Diagnocat has in place a written agreement with the Subprocessor that requires it (a) to process Patient Data only in accordance with the Terms and this Addendum, and (b) where such Subprocessors are located abroad, to undertake to comply with the applicable Data Protection Law, to implement sufficient means to secure the data and not to transfer the data to any other party and (ii) we remain liable to Customer for ensuring that our Subprocessors process Patient Data in accordance with the Terms and this Addendum.

3.2. **Data transfers:** Customer acknowledges that Diagnocat may transfer Patient Data for processing to one or more of its affiliates or third party subprocessors in the course of providing the SaaS to the Customer, provided that such affiliate or Subprocessors undertake to comply with the applicable Data Protection Law, to implement sufficient means to secure the data and not to transfer the data to any other party.

3.3. **Customer Personal Data:** Section 1.13 applies. Where the applicable Data Protection Law of Israel requires consent for any processing of Customer Personal Data (for example, for direct marketing), Diagnocat will obtain such consent separately, and Customer may refuse or withdraw it at any time without affecting the provision of the SaaS, except where the processing is necessary to provide it.

3.4. **Registration:** Customer shall register its databases with, or notify them to, the Israeli Privacy Protection Authority, and appoint a data protection officer, where required under the Protection of Privacy Law, 5741-1981, as amended by Amendment No. 13 (in force from 14 August 2025). Diagnocat will apply security measures that meet the Protection of Privacy Regulations (Data Security), 5777-2017 to the Patient Data it processes for Customer and will assist Customer in reporting any severe security incident to the Privacy Protection Authority where required.

4. **Additional Terms applicable to Russia:**

4.1. For Customers located in Russia, "**Data Protection Law**" means applicable data protection or privacy laws or regulations in the country in which the Purchaser practices dentistry and/or orthodontics with respect to its patients, including, without limitations, the Federal Law "On Personal Data" of 27 July 2006 No. 152-FZ (as amended) ("Personal Data Law"), the regulatory acts of the Russian Federation on personal data processing, as well as any applicable provisions of the EU General Data Protection Regulation (2016/679) and the Privacy and Electronic Communications Directive (2002/58/EC) (each as amended), and including US Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations made thereunder, including the Standards for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Parts 160 and 164, the security and privacy provisions of the American Recovery and Reinvestment Act of 2009.

4.2. **Subprocessing:** Customer agrees that Diagnocat may subcontract its processing of Patient Data to third parties ("Subprocessors") provided that: (i) Diagnocat has in place a written agreement with the Subprocessor that requires it (a) to comply with the principles and rules of personal data processing provided for by Personal Data Law, (b) to respect the confidentiality of personal data, (c) to take the necessary measures aimed at ensuring the fulfillment of obligations provided for by Personal Data Law.

4.3. **Data transfers:** Customer acknowledges that Diagnocat may transfer Patient Data for processing to one or more of its affiliates or third party subprocessors in the course of providing the SaaS to the Customer, including those located outside of Russian Federation, provided that such affiliate or Subprocessors undertake to comply with the applicable Data Protection Law, to implement sufficient means to secure the data and not to transfer the data to any other party, unless otherwise is permitted under the Data Protection Law. The Customer shall provide for signing by each Patient the consent for such cross-boarder transfers where it is required under the Data Protection Law.

4.4. **Customer Personal Data:** Section 1.13 applies. Where the Personal Data Law requires consent for the processing of Customer Personal Data or for its cross-border transfer, such consent will be obtained in the form required by the Personal Data Law; where Customer is an entity, Customer shall obtain such consent from its employees and agents whose data it provides to Diagnocat. Consent may be withdrawn at any time by written notice to Diagnocat at its address specified herein. Customer has the right to access their Personal Data processed by Diagnocat and to request its correction, blocking or erasure, if personal data is incomplete, outdated, inaccurate, illegally obtained or is not necessary for the stated purpose of processing, as well as to take measures provided by law to protect their rights. For this purpose, Customer may contact Diagnocat at the address specified herein.

4.5. **Data localization:** Where Customer processes Personal Data of citizens of the Russian Federation through the SaaS, Customer, as the Data Controller, shall ensure compliance with the applicable data localization requirements under Article 18(5) of Federal Law No. 152-FZ. Diagnocat will host and store Patient Data of Russian Customers in databases located within the Russian Federation using VK.Cloud and ensure that the relevant processing operations comply with applicable data localization requirements. Where cross-border transfers of Patient Data are contemplated, Customer shall submit any notification required to Roskomnadzor under Article 12 of Federal Law No. 152-FZ before such transfers take place and comply with applicable transfer restrictions. Diagnocat will provide Customer with reasonable assistance and information necessary to meet these requirements and will carry out cross-border transfers on Customer's behalf only in accordance with Customer's documented instructions and applicable Data Protection Law.

5. **Additional Terms applicable to Australia:**

5.1. **Australian Privacy Principles:** Diagnocat will handle Patient Data as if it were bound by the Australian Privacy Principles (“APPs”). It will not use Patient Data for direct marketing and will protect it as APP 11 requires.

5.2. **Data breaches and overseas disclosure:** Diagnocat will support Customer’s assessment and notification of eligible data breaches under the Notifiable Data Breaches scheme, and Customer’s obligations under APP 8 for disclosures of Patient Data overseas. Where state or territory health records laws apply, Diagnocat will also comply with them.

6. **Additional Terms applicable to Canada:**

6.1. **PIPEDA:** Diagnocat will use Patient Data only for the purposes for which it was transferred, and will protect it as PIPEDA Principle 4.7 requires.

6.2. **Québec:** Where Québec’s Act respecting the protection of personal information in the private sector applies: (a) this Addendum is the written mandate under section 18.3 of that Act; (b) Diagnocat will promptly notify Customer’s person in charge of the protection of personal information of any confidentiality incident; and (c) Diagnocat will provide the

information Customer needs for its section 17 assessment before Patient Data is communicated outside Québec.

6.3. **Provincial health information laws:** Where Customer is a health information custodian, for example under Ontario's Personal Health Information Protection Act (PHIPA), Diagnocat will meet the obligations that law places on agents and electronic service providers.

7. **General Terms**

7.1. **Confidentiality.** Each Party must keep the information it receives about the other Party and its business in connection with this Addendum ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

7.2. **Notices.** All notices and communications given under this Addendum must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the Terms or at such other address as notified from time to time by the Parties changing address.

7.3. **Processor liability and Insurance.** Diagnocat remains responsible for its processing of Patient Data in accordance with applicable Data Protection Law and the allocation and limitations of liability set out in the Terms, except for any liability that cannot be limited or excluded under applicable law. Diagnocat maintains liability insurance coverage appropriate to its role as a processor, as required by applicable law and industry practice. Diagnocat will provide evidence of such insurance coverage on Customer's reasonable request.