



END-USER LICENSE AGREEMENT

LAST UPDATED ON March 28th, 2024.

These EULA govern the terms and conditions applicable to the use of the Solution between **Vade** and the **Customer**.

Article 1 - Definitions

Whenever they are used in the Agreement or in connection with its performance, with their first letter capitalized, whether in singular or plural form, the following terms shall have, between the Parties, the meaning defined below:

Affiliate(s) means an entity that is directly or indirectly controlled by, or under common control with a Party through ownership, contract or otherwise. "Control" means that more than fifty percent (50%) of the controlled entity's shares or ownership interest representing the right to make decisions for such company are owned or controlled, directly or indirectly, by the controlling entity.

Add-on means any facultative feature associated to the Solution to which the Customer may subscribe.

Administrator means one of the Customer's employees or a third party acting on behalf of the Customer and designated accordingly by the Customer on the Management License Portal.

Agreement means this EULA, the DPA and the SLA.

API means an application programming interface.

Beneficiary(ies) means the Customer and/or its Affiliates which use the Customer Tenant.

Purchase Agreement means the commercial terms and conditions applicable to the Commercial Offer and signed between the Customer and a reseller or partner of Vade's solution, or Vade. For the avoidance of doubt, the Purchase Agreement between Customer and reseller or partner is not part of the Agreement.

Commercial Offer means the commercial package defined by Vade and distributed indirectly, or exceptionally directly, by Vade and specified in the Management License Portal.

Confidential Information means any information that a Party (or an Affiliate) discloses or makes accessible to the other Party in the context of the execution of the EULA. It is agreed between the Parties that the Solution, the Services and the tangible or intangible elements that are included within the Solution & the Services, Personal Data, and the content of e-mails are confidential. Confidential Information expressly excludes information (a) which was already in the public domain at the date of its disclosure; (b) for which it can be demonstrated that it was already known by the other Party prior to its disclosure; (c) which has been independently developed by the other Party, as demonstrated by the other Party's records; or (d) which has been received from a third party in a lawful manner, without breach of EULA.

Customer means the owner of the tenant(s) protected by the Solution subscribed as defined in the Management License Portal.



Customer Content means any Personal Data, text, messages, materials, files, applications communications, and other information, transmitted or stored by Customer, Beneficiaries or on behalf of Customer or of Beneficiaries, through the use of the Solution.

DPA means the data processing agreement in exhibit A.

Description of the Solution means the description of the Solution on Vade website.

Environment means one installation with a unique database in a logically separated tenant environment as defined by the Administrator on the Management License Portal as the case may be.

EULA means these terms and conditions of use of Services and Solution, as well as its exhibits.

Feedback means the feedback, or suggestions, or comments provided by Customer to Vade about the Solution, or about Customer's needs in relation with the Solution and Services.

Intellectual Property Right or IPR means all intellectual property rights, regardless of form, throughout the world, including: (a) invention, discovery, patents, utility model rights, design rights (registered or otherwise), and algorithm (b) trademarks, service marks, trade dress, and other rights in designations of source or origin together with the goodwill symbolized by any of the foregoing, (c) published and unpublished works of authorship, copyrights and moral rights, (d) computer programs, operating systems, applications, firmware and other code, including all source code, object code, binary, application programming interfaces, data files, databases, protocols, specifications, (e) database rights, (e) trade secrets, and (f) methods, processes, applications, registrations, and renewals for, and all associated rights with respect to, any of the foregoing in any part of the world.

Management License Portal means the interface platform which allows the access and the management of Solution licenses by Customer's partner or Administrator.

MTA means mail transfer agent.

NFR or Not For Resale means a Solution license as defined in the Purchase Agreement which is exclusively dedicated to the Customer use, which is not for resale and used in accordance with Vade's terms & conditions.

Personal Data means Personal Data as sets forth in the Data Processing Agreement.

Professional Services means any specific service performed by Vade for the Customer in relation with the Solution such as installation, activation, training, configuration, integration, assessment, and/or optimization of the Solution.

Vade means the editor of the Solution and its Affiliates.

Service means any services provided by Vade including without limitation the filtering service, analysis of the Solution, or technical service support as defined in the description Solution.

Service account means an administrator account specific to the Tenants protected.

Service Level Agreement or SLA means the SLA as sets forth in exhibit B.



Solution means the GWS Solution, Service, Management License Portal, and any Add-on as specified in the Management License Portal and subscribed by the Customer.

GWS Solution means Vade solution and its Upgrades, but excluding any add-ons, accessible in SaaS mode from the Management License Portal and which purpose is to filter electronic messages received by the end user and block, according to the state-of-the-art technology, illegitimate messages such as cyberattacks, viruses and other dangerous threats.

Technical Documentation means the technical documentations of the Solution provided by Vade in the Management License Portal.

Tenant(s) means Customer's instance in which the Customer and/or its Beneficiaries store their digital services.

Third Party Solution means any solution, such as a software, an API or an MTA, provided by third party and/or a Beneficiary and interconnected with the Solution.

Upgrade means new releases or versions for the Solution, including the Solution's upgrades, features, fixes and patches.

User means any natural person who is authorized by the Customer and/or the Beneficiaries to use Customer's Tenant(s).

X-VADE-KEY means the security key generated by Vade and specific to each Tenant.

Article 2 - Description of the Solution

2.1 Description of the Solution – The Solution is a security solution which filters the content of emails as specified in the Description Solution. Access to the Solution is subject to the compatibility of the Customer's infrastructure with the specifications of the Solution. The technical support provided by Vade is set forth in the SLA.

2.2 Administrator – The Customer designates an Administrator who is the privileged contact and is legally authorized to act on behalf of Customer. The Administrator manages the license, configures and connects the Solution to the protected Tenant, in accordance with (i) the Technical Description, (ii) the technical notice and, (iii) the state of art of the Third-Party Solution, and (iv) the Tenant's requirements. The Administrator is in charge of maintaining the administrative information up-to-date. In the event that the Customer does not name a specific data protection officer, the Administrator is the contact person for any information relating to data protection issues.

2.3 Activation of the Solution – During the activation of the Solution, a X-VADE-KEY is provided to the Customer to activate the Solution. An X-VADE-KEY is personal to the Customer and Customer is responsible for ensuring the confidentiality of its X-VADE-KEY. The Solution is activated and configured by the Administrator through the Management License Portal in accordance with the Technical Documentation and the technical notices and state of art of the Third-Party Solution and Tenant's requirements.



For the performance of this Agreement, the Administrator shall create an Account Service granting the administrator rights and the Tenant(s) access rights to Vade and shall maintain such rights in place during the duration of this Agreement. Depending on the Solution, the Customer may elect the Environment where its Customer Content is stored. In that case, the applicable data processing measures may vary depending on the chosen Environment.

2.4 Configuration – Customer shall ensure that the configuration and interconnection of the Solution with the Tenant and the Third-Party Solution are compliant with (i) Technical Documentations, (ii) the configuration and/or recommendation of the provider of the Tenant and/or the provider of the Third-Party Solution, and (iii) industry standards and the state of the art. Customer warrants that its use of the Solution comply with the foregoing requirements. During the configuration and this Agreement, Customer or its Administrator shall define the access rights to the Solution and the different level of rights awarded to any person acting on behalf of Customer.

2.5 Upgrades - Maintenance – Customer understands that Vade may upgrade the Solution, release Add-ons, and perform Services and/or maintenance at any time and at Vade' sole discretion. If needed, and in accordance with the SLA, Vade reserves the right to interrupt the Service and/or Solution to carry out technical interventions in order to improve its Solution, Service, operations or for any maintenance operation, and shall inform the Customer in its Management License Portal or by any appropriate means before such intervention.

Article 3 - Subscription

Pursuant to the Purchase Agreement, Customer subscribes a license for the Solution through one of Vade's solution resellers or partners (hereinafter the "Partner") located in its geographic region, or exceptionally directly through Vade. In case of channel distribution, the Partner discloses the Solution and the Commercial Offer selected by the Customer in its Purchase Agreement through the Management License Portal. Vade disclaims any and all responsibilities if the Commercial Offer declared by the Partner is incorrect.

Based on the Commercial Offer or the NFR, Vade creates a X-VADE-KEY specific to such Commercial Offer or NFR.

All business conditions are governed by the Purchase Agreement and are excluded from this Agreement.

Article 4 – License

4.1 License to the Solution – Subject to the terms of the Agreement and the Commercial Offer, Vade grants to Customer exclusively for its Beneficiaries, for the duration of the Commercial Offer, a non-exclusive and non-transferable right of use of the Solutions and Services to protect its Tenants declared in the Management license portal and for internal purpose only.

4.2 Trial License – Subject to the Terms of the Agreement and the Trial Offer, Vade grants to Customer exclusively for its Beneficiaries, for the duration of the Trial Offer, a non-exclusive and



non-transferable right of use of the Solutions and Services to test the Solution protect its Tenants declared in the Management License Portal and for internal purpose only.

4.3 NFR License – Subject to the Terms of the Agreement and the NFR conditions, Vade grants to Customer exclusively for its Beneficiaries, for the duration of the NFR, a non-exclusive and non-transferable right of use of the Solutions and Services to test the Solution protect its Tenants declared in the Management license portal and for internal purpose only.

4.4 Beta test - Vade may propose Upgrades in beta test version to all or part of its Customers. Such Upgrades in Beta test version are subject to the prior approval of the according beta test terms. Vade has no obligation to release on the market such beta test.

4.5 Restriction of use – The Beneficiaries and their Users shall not (a) use the Solution and the Services for any illegal purposes, (b) intentionally upload into the Solution any material of a hazardous nature, (c) copy, duplicate, decompile, disassemble, reduce, reverse engineer, modify or attempt to obtain or perceive the source code of any component of the Solution, (d) sublicense, transfer, resell or distribute the Solution, (e) use the Solution for any commercial purpose, and/or in breach of this Agreement or (d) access or use the Services either (i) for high risk activities, or (ii) in a manner intended to avoid incurring fees, or (iii) for materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State or (iv) in a manner that breaches, or causes the breach of any export control laws, or (v) to transmit, store, or process information subject to a specific applicable law notably the law mentioned in section 5.4.

Article 5 - Requirements for using the Service

5.1 Representation – The Customer undertakes and warrants (a) that it has full power and authority to enter into the Agreement ; (b) that it has obtain the appropriate rights to represent its Administrator, Beneficiaries and/or Users , and (c) Vade and its Affiliates against any breach of the Agreement by its Beneficiaries and/or Users, and (d) that it has all the licenses and rights necessary to comply with these terms and conditions and to carry out the Agreement in accordance with the applicable rights, in particular with regard to intellectual property and Personal Data.

Customer shall prevent and stop any unauthorized use of the Solution and/or Service and notify Vade immediately of any unauthorized use of or access to the Solution and/or Service.

The Customer undertakes to comply with Vade’s documentation and configuration. In this respect, the Customer agrees not to modify the configuration recommended or required or carried out by Vade.

5.2 Non-use in territories under international sanctions – Customer agrees to comply with all applicable export laws and regulations of the United States, the European Union, the United Kingdom and Japan, including without limitation the Export Administration Regulations of the U.S Department of Commerce, Bureau of Industry and Security and the embargo and trade sanction programs administered by the U.S. Department of Treasury, Office of Foreign Assets Control. Customer will not nor cause the export, re-export, resale, diversion, directly or indirectly, of any export-controlled items, software, or technology to any country or entity for which the Government of the United States or other applicable countries requires an export license or other



governmental approval without first obtaining such license or approval. Customer represents and warrants that neither Customer nor its agents are identified on any government export exclusion lists, including but not limited to the U.S. Denied Persons, Entity, and Specially Designated Nationals Lists. Notwithstanding the foregoing, Customer shall comply with any Vade policy that would restrict the export, re-export, resale, diversion, directly or indirectly, of Vade Solutions or of Vade Services.

5.3 Data protection - In carrying out the Agreement, the Customer undertakes to comply with the rights relating to the protection of Personal Data. In this respect, the Customer acknowledges and warrants that (i) it has all the rights necessary for Vade to process the Personal Data of Users, in accordance with the Data Protection Agreement and the privacy policy, and that (ii) it shall inform Users, directly or indirectly, of the data processing carried out by Vade.

5.4 Non-compliance HIPAA - PCI - COPPA – The Customer shall not use the Solution and Services to process any Personal Data subject to the Health Insurance Portability and Accountability Act of 1996 as it may be amended and any regulation issued under it, Payment Card Industry Data Security Standard and Children's Online Privacy Protection Act ("**Excluded Regulation(s)**"). Consequently, the Customer undertakes that, during the Agreement, no data subject to Excluded Regulation(s) will be processed, including but not limited to health data, banking data, and data relating to children under the age of 13. In the event of processing of data subject to these Excluded Regulations, the Customer shall immediately stop the processing operations and immediately notify Vade.

5.5 Export Law - The Customer shall not violate any applicable export control laws or regulation including export, re-export or use, directly or indirectly (including via remote access), any part of the Solution, Confidential Information or services in a manner, or to or for any person or entity, for which a license or other authorization is required under export control laws or regulation without the obtention of license or authorization.

5.6 Compliance with anti-corruption regulations - The Customer undertakes to comply with any applicable anti-corruption, anti-bribery and/or anti-money laundering laws in particular, but without limitation, under criminal law, the Japanese Law No. 47, known as "UCPA", the U.S. Foreign Corrupt Practices Act of 1977, the French Law n°2016-1691 of December 9, 2016 on transparency, the fight against corruption and modernization of economic life (Loi Sapin II), the United Kingdom Bribery Act, 2010, known as "UKBA" and with the OECD Convention on Combating Bribery and not to use the Solution license or the NFR license to procure an unjustified advantage for any third party.

5.7 No benchmark - The Customer, on its own behalf and on behalf of its Beneficiaries, its Users or any third party having a relationship with Customer, undertake to not disseminate directly or via a third party any results of the performance of the Agreement and/or Solution, comparative or compatibility benchmark tests or any assessment of the Solution/Services.

Article 6 – Warranties

6.1 Disclaimer – THE SOLUTION IS A SECURITY SOLUTION PROVIDED "AS IS". THEREFORE, THE CUSTOMER EXPRESSLY ACKNOWLEDGES AND AGREES THAT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE USE OF THE SOLUTION AND ANY SERVICES PERFORMED BY OR



ACCESSED THROUGH THE SOLUTION IS AT CUSTOMER'S SOLE RISK AND THAT THE ENTIRE RISK IS LIMITED TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT.

TO THE EXTENT PERMITTED BY THE APPLICABLE LAW AND EXPRESSLY STATED BY VADE IN THE AGREEMENT, VADE (A) MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, STATUTORY OR IMPLIED (IN FACT OR BY OPERATION OF LAW), REGARDING THE SOLUTION, SERVICE, OR ANY MATTER WHATSOEVER; AND (B) DOES NOT WARRANT THAT THE SOLUTION, SERVICE OR ANY PROFESSIONAL SERVICES ARE OR WILL BE ERROR-FREE, MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY PARTICULAR RESULTS, OR BE TIMELY OR SECURE. VADE EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT WITH RESPECT TO THE SOLUTION, SERVICE, SUPPORT AND ANY PROFESSIONAL SERVICES. THE SOLUTION MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT TO THE USE OF THE INTERNET, MTA, API OR ELECTRONIC COMMUNICATIONS. VADE IS NOT RESPONSIBLE FOR DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE, LOSS OR LIABILITY RESULTING FROM SUCH PROBLEMS NOT CAUSED BY VADE.

CUSTOMER AGREES THAT ITS SUBSCRIPTION TO THE SOLUTION, SERVICE AND FEES DUE OR PAID UNDER PURCHASE AGREEMENT ARE NEITHER CONTINGENT ON THE DELIVERY OF ANY FUTURE FUNCTIONALITY OR FEATURES, NOR BASED ON ANY ORAL OR WRITTEN COMMENTS REGARDING ANY FUTURE FUNCTIONALITY OR FEATURES.

6.2 Third-party Warranty – Customer understands and agrees that any additional or different warranty provided by a third party including but without limitation, Vade's distributor, agent, supplier, authorized re-sellers is not applicable to Vade. For the avoidance of doubt, Vade disclaims any and all liability related to any additional or different warranty provided by a third party.

Article 7 - Intellectual property

7.1 Ownership of the Solution - All intellectual property rights inherent to the Solution and the Service including, but without limitation, the databases used by Vade, the MTAs, the policy used for the MTAs, and the APIs are owned or controlled by Vade. Except for the license hereby granted, the Customer acquires no intellectual property rights over the Solution and the Service.

7.2 Customer's Content - Any intellectual property rights in the content of the emails or protected material are owned or controlled by the Customer. Notwithstanding the foregoing, the Customer grants to Vade, for the duration of the intellectual property rights, a worldwide, non-exclusive, sub-licensable, assignable, and transferable license to reproduce and use the content of the emails in order to improve its solutions, products and services and to carry out the Services.

7.3 Feedback - If the Customer, directly or indirectly, in particular through its Beneficiaries, Users, Administrator, provides Vade with Feedback concerning the Solution or Services, Customer acknowledges and agrees that Vade may use the Feedback, and Customer hereby irrevocably assigns to Vade all unrestricted, perpetual, irrevocable, non-exclusive, fully-paid, royalty-free, transferable sub licensable rights, title and interest in and to such Feedback, to exploit the Feedback in any manner, for any purpose, and on any territory.



Article 8 – Third-Party Solution

8.1 Use of Third-Party Solution – Customer itself or a third-party on behalf of Customer may interconnect a Third-Party Solution with the Solution. Any and all Third-Party Solution used and connected by Customer shall be (i) compliant with Vade technical and security requirements and/or at least with the security industry standard and Technical Documentation, (ii) subject to first obtaining all appropriate rights to use such Third-Party Solution. Customer warrants Vade against any action relating to the use or connection of any Third-Party Solution with the Solution in particular but without limitation against intellectual property infringement.

8.2 Third-party Solution under open-source license – Customer ensures that Third-Party Solution or third-party element that are used with or interconnected with the Solution is not subject to copyleft open-source licenses. Customer agrees to comply with any Vade policies and their updates regarding Third-party Solution under open-source license.

8.3 No warranty on Third-Party Solution – Vade expressly excludes its responsibility if Customer uses Third-Party Solution or third -party elements in connection with the Solution.

Article 9 - Confidentiality

9.1 Obligation of confidentiality - Subject to Article 9.2, each Party undertakes to use the Confidential Information only in order to carry out its obligations hereunder. Each Party warrants the confidentiality of the Confidential Information and shall refrain from disclosing it to anybody other than those entitled to, whether employees, Beneficiaries, Users or service providers, and shall take all appropriate technical and organizational measures to protect the confidentiality of Confidential Information.

9.2 Legal Obligation - Pursuant to an order or request from a governmental authority, Court or agency (hereinafter a "**Request**"), Vade and its Affiliates may disclose Confidential Information subject to disclosing only such information that is strictly necessary to comply with the Request and, shall inform the authority of the confidentiality of the requested Confidential Information.

Article 10 - Personal data

10.1 Parties as Controller – Each Party declares and warrants the other one to comply with and fulfill its obligations regarding Personal Data such as resulting from the applicable law as well as the General Data Protection Regulation (EU) 2016/679 (GDPR) and in particular to comply with the principles relating to the processing of Personal Data. Within the limits of this EULA and for the management of the contract and the improvement of the solution and service, Vade, as data controller, processes Personal Data in accordance with its privacy policy. The privacy policy may be updated at any time by Vade.

The Customer acknowledges and agrees that Vade (i) can always ensure that the use of the Solution is appropriate, check licenses and/or (ii) may report to its commercial partner the quantity of licenses. In particular, Vade (and as the case may be, together with an appointed reputable external auditor) may upon a reasonable notice and at reasonable time intervals and for a reasonable duration, verify any data regarding access and use of the Solution and the correspondence between the scope of the license subscribed and the current use.



10.2 Use of the Solution – As controller of Personal Data processes during the use of the Solution and Services, Customer ensures that it complies with applicable law and ensures that all formalities necessary for the processing of Personal Data for the use of the Solution and the execution of these EULA have been carried out. Customer shall comply with the applicable principles governing the processing of Personal Data and the rights of Personal Data. Furthermore, in this context, Customer subcontracts to Vade the processing of Personal Data for which it has responsibility and rights for the performance of the Agreement. Subcontracting is carried out by Vade in accordance with the Data Processing Agreement.

Article 11 – Indemnification

11.1 Vade Indemnification - Vade shall indemnify and defend Customer, its beneficiaries, and Users and each of their respective officers, directors, employees, agents, successors and assigns against direct damage for any third-party claim asserting that the Solution or Service, when made available to Customer by Vade and when properly used for the purpose and in the manner specifically authorized by this Agreement, infringes any IPR, provided that Customer (i) has used the Solution and/or Service in accordance with the Agreement, (ii) has notified Vade within ten (10) calendar days from the receipt of the claim, (iii) accepts to give Vade sole control over the defense or the settlement of the claim, (iv) reasonably cooperates with Vade for the defense of the claim; (v) does not make any acknowledgment, concession, consent or settlement with respect to the claim (except with the written consent of Vade). Vade shall not indemnify Customer or its Beneficiaries or its Users in the event that the claim arises on the basis of (i) the use of a Third-Party Solution or a third-party element in connection with the Solution, or (ii) the modification of the Solution by Customer, its Beneficiaries or its Users, or (iii) the use of the Solution in violation of the Agreement. The indemnification is limited to the higher amount between (i) the amount of the fees paid by Customer for the Commercial Offer during the last twelve (12) months or (ii) to twenty five thousand (25 000) dollars for any Customer located in the USA, Canada or Japan, and to twenty five thousand (25 000) euros for any other Customer.

In the event of a claim or a threat of a claim, Vade may at its option and expense: (i) modify or replace all or the allegedly infringing part of the Solution or Service so that it is no longer allegedly infringing, provided that the modification or replacement does not result in a material change of such Solution or Service, or (ii) procure for Customer the right to continue using the allegedly infringing part of the Solution or Service ; or (iii) remove all or part of the allegedly infringing of the Solution or Service.

11.2 Customer Indemnification – Customer shall indemnify and defend each of Vade, its Affiliates, and each of their respective officers, directors, employees, agents, successors and assigns against any third-party claim resulting or arising from a claim, which in whole or in part, directly or indirectly, alleged (a) an infringement of intellectual property rights other than the ones referred to in Section 11.1, or (b) an infringement of any third party rights regarding its Data Content. Vade shall have the right to monitor the progress of the dispute and settle the claim for the part that concerns Vade or its Solution or Service.

11.3 Commune provision – The remedies provided in this Section 11 are the sole remedies for any intellectual property infringement.



Article 12 - Liability

NOT WITHSTANDING THE FOREGOING, IN NO EVENT EITHER PARTY SHALL BE LIABLE FOR COST OF PROCUREMENT OF SUBSTITUTE GOODS, LOSS OF REVENUE, LOST PROFITS, LOSS OF BUSINESS, TRADING LOSSES, INCURRED DISTRIBUTIONS, LOSS OF OPPORTUNITY OR FOR ANY OTHER SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED.

IN NO EVENT VADE SHALL BE LIABLE FOR ANY ACTION, EVENT ARISING OUT THE PURCHASE AGREEMENT BETWEEN CUSTOMER AND PARTNER.

TO THE EXTENT PERMITTED BY THE APPLICABLE LAW AND EXCEPT THE INDEMNIFICATION PROVISIONS SET FORTH IN SECTION 11, IN NO EVENT THE CUMULATIVE LIABILITY OF VADE AND/OR ITS AFFILIATES SHALL EXCEED THE LESSER AMOUNT BETWEEN (I) THE AMOUNT PAID BY CUSTOMER FOR COMMERCIAL OFFER DURING THE LAST TWELVE (12) MONTHS OR (II) TO TWENTY FIVE THOUSAND (25 000) DOLLARS FOR ANY CUSTOMER LOCATED IN THE USA, CANADA AND JAPAN AND TWENTY FIVE THOUSAND (25 000) EUROS FOR ANY CUSTOMER

Article 13 - U.S. Government Customer

Each of the components that constitute the Solution, is a “commercial item” as that term is defined at 48 C.F.R. 2.101, consisting of “commercial computer software” and/or “commercial computer software documentation” as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the Solution with only those rights set forth herein. If Solution is acquired for or on behalf of the U.S. Government, then it is recognized and agreed that the Solution: (i) was developed at private expense; (ii) was not required to be originated or developed under a Government contract; and (iii) was not generated as a necessary part of performing a Government contract. United States government agencies and entities and others acquiring under a United States government contract shall have only those rights, and shall be subject to all restrictions, set forth in this Agreement.

Article 14 - Modification

For Customer located in the geographic region of the USA, Canada and Japan:

Vade may at any moment modify the Agreement without any prior notification. Vade informs the Customer by any electronic tool of such modification.

For Customer located in the geographic region of the European Union, the European Economic Area, the United Kingdom and the rest of the world:

Vade may, at any moment and without prior notification, modify the Agreement by an informative notice if the purpose of the modification does not create a material modification and/or is aimed at (i) ensuring the compliance of the Agreement with the law and/or requirements imposed by a regulatory authority; (ii) correcting an error; (iii) clarifying some provisions. In case of a material modification, a notice shall be sent one (1) month before the implementation of such material modification. Customer shall have then one (1) month to terminate the Agreement. Vade may modify the Agreement without any notification if the modification is not material or if such modification is made in favor of Customer.



Article 15 - Effective date - Term - Termination

15.1 Effective Date and Duration - The EULA and the licenses rights set forth in section 4 enter into force on the approval date of such EULA. For the avoidance of doubt, if the Customer does not accept the EULA, the license rights set forth in section 4 are null and void.

15.2 Expiration or Suspension or Termination for Customer

15.2.1 Termination for the Breach of Agreement: Either party (the “Non-breaching Party”) may terminate this Agreement, effective immediately upon written notice to the other party (the “Breaching Party”), if the Breaching Party breaches any provision of this Agreement and does not cure the breach within thirty (30) calendar days after receiving written notice thereof from the Non-breaching Party. Notwithstanding the foregoing, in case of material breach of the Customer in particular Sections 4, 5, 8.2, 13, Vade may terminate the Agreement immediately.

15.2.2 Expiration; Suspension or Termination arising out from the management of Customer Purchase Agreement: The expiration, suspension or termination of Customer Purchase Agreement leads to the expiration, suspension, or termination of this Agreement without any delay and compensation from Vade. Vade expressly disclaims any responsibility resulting from the expiration, suspension or termination arising out from this section.

15.2.3 Emergency Suspension. If Customer, or a third party on behalf of Customer, uses the Solution or Service in breach of Section 4.5, 2.4 and 8, Vade may immediately suspend Customer’s use of the Solution or Services to protect the Solution and the third-party customer.

15.3 Consequence of Expiration or Termination or Suspension

The expiry or termination of the Agreement shall occur without prejudice to the rights or liabilities acquired by the Parties or to which they are subject and to the survival of all provisions having by nature or as specified herein an effect after the termination of this Agreement, including to but not limited to provisions for confidentiality, Personal Data, intellectual property, license fees (if applicable) or liability. Upon suspension or termination or expiration of this Agreement for any reason, any amounts owed to VADE under this Agreement before such termination or expiration will be immediately due and payable, all licensed rights granted in this Agreement will immediately cease to exist, and Customer must promptly discontinue all further use of VADE’s IPR and all further use of the Solution.

Customer understands and agrees that Vade shall discontinue any Services and notably the MTA (if any) in case of suspension, termination or expiration of the Agreement. In consequence, if the Customer does not modify the configuration of Customer’ system, the Customer understands that it may not receive its electronical mail anymore.

Article 16 – Change of Vade’s channel network

If Customer’s distributor and/or partner loses the right to resell Vade Solution, Vade shall inform Customer that in order to continue to benefit from the Solution, Customer shall opt for a new distributor and/or partner within thirty (30) calendar days from the information, otherwise, at the end of such delay, the Agreement will be terminated. In the event of a termination of the Agreement as per this section, section 15.3 shall be applicable.



Article 17 - Applicable law - Jurisdiction

For Customer located in the geographic region of the European Union, the European Economic Area, the United Kingdom:

This Agreement is governed exclusively by French law, to the exclusion of conflict of the rule of law. The Parties have also decided not to apply the United Nations Convention on Contracts of the International Sale of Goods (CVIM) to this Agreement. Any dispute, whether contractual or not, arising out of or in connection with this Agreement (including any question regarding its existence, validity or termination) shall first be settled amicably by the Parties. In the event that the dispute cannot be settled amicably within thirty (30) calendar days of disclosure of the dispute from the receipt date of the registered letter with acknowledgement, exclusive jurisdiction is given to the Commercial Court of Paris.

For Customer located in the geographic region of the USA:

This Agreement is governed exclusively by California law, to the exclusion of conflict of the rule of law. The Parties have also decided not to apply the United Nations Convention on Contracts of the International Sale of Goods (CVIM) to this Agreement. Any dispute, whether contractual or not, arising out of or in connection with this Agreement (including any question regarding its existence, validity or termination) shall first be settled amicably by the Parties. In the event that the dispute cannot be settled amicably within thirty (30) calendar days of disclosure of the dispute from the receipt date of the registered letter with acknowledgement, exclusive jurisdiction is given to the courts of the state of California, county of San Francisco.

For Customer located in the geographic region of Canada:

This Agreement is governed exclusively by Quebec law, to the exclusion of conflict of the rule of law. The Parties have also decided not to apply the United Nations Convention on Contracts of the International Sale of Goods (CVIM) to this Agreement. Any dispute, whether contractual or not, arising out of or in connection with this Agreement (including any question regarding its existence, validity or termination) shall first be settled amicably by the Parties. In the event that the dispute cannot be settled amicably within thirty (30) calendar days of disclosure of the dispute from the receipt date of the registered letter with acknowledgement, exclusive jurisdiction is given to the courts of the state of Montréal, Quebec (Canada).

For Customer located in the geographic region of Japan:

This Agreement is governed exclusively by Japanese law, to the exclusion of conflict of the rule of law. The Parties have also decided not to apply the United Nations Convention on Contracts of the International Sale of Goods (CVIM) to this Agreement. Any dispute, whether contractual or not, arising out of or in connection with this Agreement (including any question regarding its existence, validity or termination) shall first be settled amicably by the Parties. In the event that the dispute cannot be settled amicably within thirty (30) calendar days of disclosure of the dispute from the receipt date of the registered letter with acknowledgement, exclusive jurisdiction is given to the Tokyo District Court as exclusively agreed jurisdictional court in the first instance.



Article 18 - General provisions

18.1 No Agency - The Parties are independent contractors and nothing in this Agreement shall be used nor interpreted as establishing any relationship of association, agency, partnership, joint-venture, employment between the Parties. Neither Party shall have the right to present itself as an agent or to have power to bind the other Party, to incur any obligation on its behalf without the prior and written consent of the other Party.

18.2 Proof - The Parties agree that the data, information and elements registered and/or stored by Vade regarding the use of the Solution and the sales of the Solution shall be deemed to be element of proof between the Parties.

18.3 Waiver - Any waiver or failure to enforce any provision of this Agreement shall not be used to pretend nor be interpreted as a waiver of any other provision or of such provision on any other occasion.

18.4 Severability - If any provision of this Agreement is, for any reason, held to be invalid or unenforceable, the other provisions shall remain in force and effect. The Parties shall agree upon necessary amendments to such invalid or unenforceable provision in order to validly achieve the same effect to the maximum extent permitted by law.

18.5 Force majeure - Neither party shall be liable for or considered in breach of this Agreement due to any failure to perform its obligations as result of a Force Majeure, except for payment obligation (if any). For the purpose of this Agreement, "Force Majeure" means, in relation to either Party, or in relation to Vade's providers, any event or circumstance beyond the reasonable control of that Party and which hinders the proper performance of such Party's obligations hereunder (e.g. any strikes, lockouts or other form of industrial actions, fires, flood, earthquake, storm or other like event, explosions, wars, civil commotions, riots, sabotages, lockdown, theft or criminal misconduct by unrelated third party, perturbation or congestion of telecommunications networks, act of Gods, act of any military, civil or regulatory authority, change of any law or regulation, unavailability of supplies or other cause, act of terrorist, any legal restrictions to the provision of telecommunications services and, in general, events that required the application of local or national plans to maintain the continuity of telecommunications services, etc).

18.6 Subcontract - Assignment – Vade may use subcontractors. Vade remains responsible for fulfilling the obligations assumed by Vade even if subcontractors are appointed. Vade is entitled to transfer rights and obligations in whole or in part to its Affiliates. The Customer may not assign or transfer the Agreement, contractual rights or obligations to third parties without prior written consent of Vade. Any purported assignment or delegation in violation of this Section is null and void. No assignment or delegation shall relieve the Customer of any of its obligations under the Agreement.

18.7 Reference – Customer accepts that Vade and Vade's Affiliates may use its name as reference. Therefore, Customer grants to Vade and Vade's Affiliates, for the worldwide and duration of the Agreement, the right to use, represent Customer's name and logo as reference. If Vade or Vade's Affiliates use the name or logo of Customer, Vade commits not to infringe the reputation or the image of the Customer.



18.8 Conflict of Terms - This Agreement is the final, complete and exclusive agreement set between the Parties with respect to the subject matter hereof and supersedes and merges all prior discussions between the Parties with respect to such subject matters. No other similar document that may be issued by Customer in connection with this Agreement will modify this Agreement. No amendment to this Agreement will be effective unless it is evidenced by a written amendment signed by each of the Parties, expressly stating that it amends this Agreement. In case of contradiction, the Agreement prevails over its Exhibits.

18.9 Conflict of languages - Any translation of this EULA from the English language is made solely for local requirements and in the event of a dispute between the English and any non-English versions, the English version of this EULA shall prevail.

18.10 Notice – Each Party delivers all notices in French or in English to the other Party by an email with an acknowledgement of receipt to the following email addresses:

- For Customer : to the email address provided on the Management License Portal
- For Vade : legal-contracts@vadecure.com

Customer agrees that Vade may modify this section without prior notice to implement a digital solution which allow notification between Customer and Vade. In this case, any and all communication or notices will be delivered using such communication digital tool.



EXHIBIT A – DATA PROCESSING AGREEMENT

LAST UPDATED ON March 28th, 2024.

The purpose of this data protection agreement (the "Agreement"), signed between Vade and the Tester in accordance with article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to the protection of individuals with regard to the processing of Personal Data and the free movement of such data, and repealing Directive 95/46/EC ("GDPR"), is to define the conditions under which the Data Processor processes, upon the instructions of the Data Controller, Personal Data as defined in the GDPR.

This Agreement is part of the GTU signed between the Parties for the performance of services by the Data Processor for the benefit of the Data Controller.

1. DEFINITIONS

As used in this Agreement, the following terms shall have the following meanings (such meanings to be equally applicable to both the singular and plural forms of the terms defined):

Personal Data: means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Incident: refers to any security incident, of malicious origin or not, occurring intentionally or not, having the consequence of compromising the integrity, confidentiality or availability of Personal Data.

Applicable Laws: means the laws and regulations relating to the processing and protection of Personal Data applicable in the country where the Data Processor is established. Applicable Law means in particular (a) the GDPR, (b) the laws and regulations of a member state of the European Union relating to the processing and protection of Personal Data, integrating or supplementing the GDPR; (c) any other applicable law or regulation relating to the processing and protection of Personal Data under the Agreement.

Services: refers to the services provided by the Data Processor to the Data Controller and which involve Data Processing on behalf of the Data Controller.

Data Processing: means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2. PURPOSE OF THE AGREEMENT

The purpose of this Agreement is to organize the processing of Personal Data in the context of the performance of the Services provided by the Data Processor to the Data Controller.



3. COMPLIANCE

The Parties agree to comply with the Applicable Laws as defined in this Agreement.

If the Data Processor believes that all or part of the Data Controller's instructions constitute or may constitute a violation of the Applicable Laws, it shall inform the Data Controller promptly in order to obtain modified instructions, except where the Applicable Laws prohibit the provision of such information.

The Data Controller shall adapt the instructions, with the reasonable assistance of the Data Processor, to ensure compliance with the Applicable Laws. These changes are likely to have a substantial impact on the performance of the Services and may require, in particular, a review of the scope and financial conditions of the provision of the Services. In this case, the Parties shall negotiate in good faith the necessary revisions, including the deadline for implementing the changes requested by the Data Controller.

The Data Controller expressly acknowledges and accepts that the Data Processor shall not be bound by instructions violating the Applicable Laws. The Data Processor reserves the right to suspend the performance of the Services until the Data Processor's instructions are modified to comply with the Applicable Laws. In such a case, the Data Processor shall inform the Data Controller of the implementation of the suspension, no later than the day of this suspension.

Notwithstanding the foregoing, the Parties acknowledge that the Data Processor cannot be held liable for a violation of the Applicable Laws when processing Personal Data in compliance with the instructions of the Data Controller.

The Data Controller shall ensure that the Data Processing entrusted to the Data Processor has an appropriate legal basis and that the data subjects have previously given, when it is required, their consent to the Data Processing in compliance with the Applicable Laws.

4. OBLIGATIONS OF THE DATA PROCESSOR

The Data Processor acknowledges and agrees that it shall only process Personal Data upon the written instructions of the Data Controller as set out in **Exhibit 1** of this Agreement. Accordingly, the Data Processor undertakes not to use the Personal Data of the Data Controller for purposes other than those indicated by the Data Controller, or for the Data Processor's own activity or for that of a third party.

If the Data Processor can't comply with the instructions of the Data Controller for any reason, other than non-compliance with the legal obligations of these instructions, the Data Controller shall be informed promptly. In such a case, the Parties shall discuss the modifications that the Data Processor would agree to implement or that the Data Controller could apply to its instructions.

The Data Processor ensures that its authorized personnel have receive an appropriate training and has been made aware of the applicable security procedures before processing Personal Data entrusted by the Data Controller. The Data Processor shall furthermore ensure that its authorized personnel in charge of Data Processing is bound by an appropriate obligation of confidentiality.



The Data Processor further agrees:

- that the technical and organizational security measures described in **Exhibit 2** are based on the instructions and information received from the Data Controller as set out in **Exhibit 1**; and,
- that the technical and organizational security measures are adequate considering the processing risks and the defined Data Processing purposes. In particular, the Data Processor undertakes not to reduce the overall security of the Data Processing during the term of this Agreement without the prior consent of the Data Controller; and,
- to provide the Data Controller with reasonably accessible and relevant information concerning the Data Processing carried out, such as the information necessary to conduct a data protection impact assessment on the Data Processing; and,
- to keep a record of processing activities of all categories of Data Processing activity carried out on behalf of the Data Controller and to make such record available to the Data Controller upon request; and,
- to comply with the principles of data protection by design and by default; and,
- to provide the Data Controller with the reasonable cooperation and assistance to answer to requests from data subjects, in particular the rights of access, rectification, erasure, restriction or portability; and,
- to provide the Data Controller with all the documentation justifying the compliance with the Data Processor's obligations as per this Agreement; and,
- to deal with Incidents in accordance with this Agreement, and in particular in accordance with the Section "Management of Incidents".

5. OBLIGATIONS OF THE DATA CONTROLLER

The Data Controller ensures that it has all the necessary consents and rights to authorize the Data Processor to process the Personal Data on its behalf and in accordance with this Agreement. If the Data Controller acts on behalf of a third party, the Data Controller shall guarantee to the Data Processor that the instructions provided to the Data Processor concerning the Processing of Data, including the designation of the Data Processor for the performance of the Services, have been authorized by the Data Controller's own data controller.

The Data Controller provides the Data Processor, within the **Exhibit 1** of this Agreement, with all the instructions necessary for carrying out the Data Processing and for creating the record of processing activities with regard to the Data Controller's Personal Data.

In the event that the Data Controller wishes to modify its instructions, it shall notify the Data Processor at least thirty (30) days in advance in order to allow the Parties to discuss the proposed modifications.

The Data Controller acknowledges that the provision of the instructions by the Data Controller to the Data Processor is necessary so that the Data Processor can adequately carry out the Data Processing.



The Data Controller is solely responsible for the Data Processing carried out by the Data Processor in compliance with the Data Controller's instructions.

The Data Controller also acknowledges that any modification of the instructions is likely to have a substantial impact on the performance of the Services and require, in particular, a review of the scope and of the financial conditions of the provision of these Services. Accordingly, the Parties shall negotiate in good faith the necessary revisions, including the deadline for implementing the modifications requested by the Data Controller.

6. MANAGEMENT OF INCIDENTS

In the event of an Incident affecting the Personal Data, the Data Processor undertakes to inform the Data Controller, within seventy-two (72) hours of becoming aware of such Incident, indicating: the nature of the Incident, the expected consequences of the Incident, the categories and the estimated number of data subjects and files concerned. This alert must be accompanied by any useful documentation to enable the Data Controller, if necessary, to notify this violation to the supervisory authority. Except as otherwise required by the Applicable Laws, the Data Processor further undertakes not to notify any Incident to a supervisory authority without the prior consent of the Data Controller.

7. TRANSFER OF PERSONAL DATA

Except as otherwise provided in **Exhibit 1** of this Agreement, the Data Processor undertakes not to process the Personal Data of the Data Controller outside the European Union without having previously obtained the written consent of the Data Controller.

If the Data Processing by the Data Processor involves a transfer of Personal Data outside the European Union, the Data Processor must first ensure that the third-party processors provide an adequate level of protection under the Applicable Laws for the Data Processing of the Data Controller's Personal Data.

The Data Processor further undertakes to ensure that any third party data processor duly authorized to process Personal Data outside the European Union has agreed to comply with the appropriate Standard Contractual Clauses for the transfer of Personal Data set by the European Commission (or any competent authority), the European Commission "Data Processor" Standard Contractual Clauses, in accordance with Decision 2021/914, and implements, where appropriate, technical measures, additional organizational and legal measures when the analysis of local laws and data protection practices reveal that they are likely to challenge the effectiveness of the warranties agreed between the Parties. If the Data Processor is unable to comply with the Standard Contractual Clauses, the Data Processor undertakes to implement alternative protections to the Standard Contractual Clauses in order to ensure an adequate level of protection of Data Controller's Personal Data.

8. SUBCONTRACTING

Unless otherwise stated in **Exhibit 1** of this Agreement, the Data Processor undertakes not to subcontract the Data Processing of the Data Controller's Personal Data.



Notwithstanding the foregoing, if the Data Processor decides to subcontract the Data Processing, then the Data Processor shall inform the Data Controller thirty (30) days before such change.

The Data Processor must impose the same obligations on the subcontractor as set out in this Agreement. This is executed through a contract or another legal act under the Applicable Law. It must be ensured that sufficient warranties are provided from the subcontractor to implement appropriate technical and organisational measures in such a manner that the Data Processing will meet the requirements of the Applicable Laws (“back-to-back” terms).

If the subcontractor fails to fulfil its data protection obligations, the Data Processor remains liable to the Data Controller for the performance of the subcontractor’s obligations.

9. EXERCISE OF RIGHTS

The Data Controller shall define the means for processing data subjects’ requests for the exercise of their rights. The Data Processor shall, in compliance with the Applicable Laws, assist as far as possible the Data Controller in the performance of its obligations in connection with the exercise of rights by data subjects.

In the event that the Data Processor receives a request from a data subject, the Data Processor undertakes not to respond directly to the request but to inform the Data Controller no later than seven (7) working days from the receipt of the data subject’s request. The Data Processor shall not be held liable for consequences that would result from a lack of response, or a response given too late by the Data Controller, to a request for the exercise of rights if such request has been duly transmitted in a timely manner by the Data Processor to the Data Controller.

10. DURATION AND TERMINATION

This Agreement shall come into force as of the last date of signature by the Parties and shall remain applicable for the duration of the provision of the Services by the Data Processor for the benefit of the Data Controller.

The Parties agree that the Section "Deletion and return of Personal Data" shall survive the expiration of the Agreement for whatever reason.

11. DELETION AND RETURN OF PERSONAL DATA

Except as otherwise requested by the Data Controller or provided by the Applicable Laws, the Data Processor undertakes to delete all Data Controller’s Personal Data on any medium whatsoever no later than one (1) month as of the end of the provision of the Services by the Data Processor for whatever reason.

Upon request by the Data Controller, the Data Processor shall provide a certificate of destruction of the Personal Data to the Data Controller.



12. MISCELLANEOUS

12.1. Contact and notifications

For the performance of this Agreement, the Parties may contact and notify the other Party at the addresses set in this Section.

For the Data Processor:

- By email: dpo@vadesecure.com
- By post: VADE, Attn: DPO, 2bis Avenue Antoine Pinay, 59510 Hem, France.

For the Data Controller:

- Via email: mentioned on the Management License Portal

12.2. Entire Agreement

This Agreement contains all the obligations of the Parties regarding to its purpose. Except as otherwise written in this Agreement, in case of contradiction (i) between any commercial contract signed between the Parties for the performance of the Services and this Agreement, this Agreement shall prevail; (ii) between this Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

No amendment to this Agreement will be effective unless it is evidenced by a written amendment signed by each of the Parties, expressly stating that it amends this Agreement.

12.3. List of Exhibits

Exhibit 1: Data Processing and instructions

Exhibit 2: Security measures



EXHIBIT 1
DATA PROCESSING AND INSTRUCTIONS

Creation	November 7 th , 2023
Last update	March 28 th , 2024
Processing activity name	VADE FOR GOOGLE WORKSPACE

FOR EUROPEAN ENVIRONMENT

Purpose

Filtering of Customer's incoming emails to block standard and sophisticated email attacks (in particular without limitation phishing, spear-phishing, malware).

Data subjects categories

Users of the Customer's email domain name.

Data categories

Name, first name, business phone number and contact information for the signature, performance or termination of the agreement;

E-mail addresses of all users of the solution.

E-mail addresses of all senders and recipients of all e-mails that are processed by the solution.

Technical characteristics, subject and contents of emails identified legitimate or "false positive" or "false negative" by the user.

Subject, links (or URLs), attached files, phone number and image links contained in all emails processed by the solution.

Are sensitive data processed?

Yes No. However, this possibility is left to the entire responsibility of the Customer and his contacts who can, themselves, decide to send or receive sensitive data through e-mails.

Data retention period

Emails are kept during 20 seconds to perform the filtration before its disclosure to the End Users or Users

Emails identified as "false positive" or "false negative" by the user are retained for seven (7) days.

The user's logs are kept for a maximum of 90 days.

The user's logs of the RBI Solution are kept for a maximum of 1 year.



Data identifying the client's representative (last name, first name, business phone number) as well as the exchanges necessary for the signature, performance or termination of the agreement, are kept for the applicable legal terms.

The IP addresses of the servers sending emails to the users of the solution, the subjects, links (or URLs), phone numbers and image links contained in the emails processed by the solution are kept for a minimum of three (3) months.

Data processors

Internal data processors

1. Tech products Department and Customer Services

Subcontractors

Solution :

1. GOOGLE CLOUD PLATFORM (for storage of the solution) – France *
2. SCALEWAY (for Solution and first backups storage) – France
3. OVH France (for Solution and second backups storage) – France

Add-on RBI

4. OODrive (RBI option – Outscale) – European Union

Support and helpdesk:

5. ZENDESK (for ticketing support) - USA
6. AIRCALL (virtual call center) – USA, UK, Germany and Vietnam

Data transfer

Are personal data transmitted outside the European Union?

Yes No

USA, UK et Vietnam only for ticketing (ZENDESK) et virtual call center (AIRCALL).

(*) personal data may be transferred outside EU by Google. There is also an inherent risk resulting from the User's use of a Microsoft ID.



EXHIBIT 2

SECURITY MEASURES

Vade currently complies with the Security Measures described in this Exhibit 2. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: Vade hosts its Service with outsourced cloud infrastructure providers (infrastructure as a service). Additionally, Vade maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement.

Vade relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: Vade hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for Tiers 3 and ISO 27001 compliance, among other certifications (like SOC 2 type 2 or ISO 27701).

Authentication: Vade implemented a uniform password policy for its products. Customers or Testers who interact with the products via the user/admin interface must authenticate before accessing non-public customer/Tester data.

Authorization: Customer/Tester Data are stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure.

The authorization model in each of Vade's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options using less privileges principle. Authorization to data sets is performed through validating the user's permissions against the profile associated with each customer data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth/SAML authorization.

ii) Preventing Unauthorized Product Use

Vade implements industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.



Static code analysis: Security reviews of code stored in Vade's source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: Vade maintains relationships with industry recognized penetration testing service providers for annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

Vulnerability testing and Patch management: Vade maintains relationships with industry recognized vulnerability testing service providers for Six annual vulnerability tests on all Vade Assets. The intent of the vulnerability tests is to identify and resolve weakness that could tamper Vade security level. Vade apply monthly security patches delivered by software or infrastructure suppliers on all components of Vade's infrastructure.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of Vade's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security Incidents and implement data security. All such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are Initiated annually. Employee roles are reviewed at least once every year.

Background checks: All Vade employees undergo a background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: Vade makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the Vade products. Vade's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Vade stores user passwords following policies that follow industry standard practices for security. Vade has implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: Vade designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Vade personnel, including security, operations, and support personnel, are responsive to known Incidents.

Response and tracking: Vade maintains a record of known security Incidents that includes description, dates and times of relevant activities, and Incident disposition. Suspected and confirmed security Incidents are investigated by security, operations, or support personnel; and



appropriate resolution steps are identified and documented. For any confirmed Incidents, Vade will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to Customer will be in accordance with the terms of the DPA or Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.9% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure.

Online replicas and backups: Where feasible, production databases are designed to be clustered on multiple instances. All databases are backed up and maintained using at least industry standard methods.

Vade's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Vade operations in maintaining and updating the product applications and backend while limiting downtime.



EXHIBIT B – SERVICE LEVEL AGREEMENT

The Service Level Agreement related to the Solution Vade for Google Workspace (“**SLA**”) is available at on Vade website.

Privacy Policy related to the Solution Vade for Google Workspace (“**Policy Privacy**”) is available at https://www.vadesecure.com/hubfs/Ressource%20Marketing%20Website/Conditions%20of%20use/PRIVACY%20POLICY%20_%20VADE%20FOR%20GOOGLE%20WORKSPACE_March%2028%2c%202024.pdf