MASTER SUBSCRIPTION AGREEMENT & DATA PROCESSING AGREEMENT

Licensee: ______________________________

Effective Date: Date of execution of this Agreement

This Master Subscription Agreement (this "***Agreement***") is made and entered into as of the above date (the "***Effective Date***") by and between Material Security Inc., a Delaware corporation ("***Material***"), and the above party (the "***Licensee***"). Capitalized terms shall have the meaning defined herein and, in the Exhibits, hereto.

In consideration of the premises and the covenants set forth in this Agreement, the parties hereby agree as follows:

1. Definitions.

1.1 "**Authorized Period**" means the time period specified in the Order Form.

1.2 "**Authorized Unit**" means the specific number of Units authorized for use with respect to the Licensed Software as specified in the Order Form.

1.3 "**Confidential Information**" means any and all non-public, confidential and proprietary information, furnished by one party to this Agreement (the "**Disclosing Party**") or any of its Representatives to the other party to this Agreement (the "**Receiving Party**") or any of its Representatives, whether orally, in writing, or in other tangible form. Without limiting the generality of the foregoing, Confidential Information may include, without limitation, that which relates to patents, patent applications, trade secrets, research, product plans, products, developments, know-how, ideas, inventions, processes, design details, drawings, sketches, models, engineering, software (including source and object code), algorithms, business plans, sales and marketing plans, and financial information. Any Confidential Information disclosed in a written or other tangible form shall be clearly marked as "confidential," "proprietary," or words of similar import. Any Confidential Information disclosed orally shall, to the extent practicable, be identified as confidential at the time of disclosure. Notwithstanding the foregoing, Confidential Information shall expressly include the terms of this Agreement, the Licensed Software and all know-how, techniques, ideas, principles and concepts which underlie any element of the Licensed Software and which may be apparent by use, testing or examination.

1.4 "**DPA**" means the Material Data Processing Agreement set forth on Exhibit B of this Agreement.

1.5 "**Derivative Work**" means a work of authorship or other development that is based on, derived from or extends, replaces, emulates, substitutes for, or exposes to third parties the functionalities of the Licensed Software, such as a revision, enhancement, modification, improvement, translation, abridgement, compression, extension or expansion or any other form in which such work may be recast, applied, transformed or adopted, and includes, without limitation, any "derivative work" as defined in the United States Copyright Act, 17 U.S.C. Section 101.

1.6 "**Intellectual Property Right**" means any of the following: (i) all letters patent and applications for letters patent throughout the world, including all patent applications in preparation for filing anywhere in the world, all reissues, divisions, continuations, continuations-in-part, extensions, renewals, and reexaminations of any of the foregoing; (ii) common law and statutory trade secrets and all other confidential or proprietary or useful information that has independent value, and all know-how, in each case whether or not reduced to a writing or other tangible form; (iii) all copyrights, whether arising under statutory or common law, registered or unregistered, now or hereafter in force throughout the world, and all applications for registration thereof, whether pending or in preparation, all extensions and renewals of any thereof and all proceeds of the foregoing; (iv) all trademarks, trade names, corporate names, company names, business names, fictitious business names, trade styles, service marks, certification marks, collective marks, logos, other source of business identifiers, prints, and labels on which any of the foregoing have appeared or appear, designs and general intangibles of a like nature, now existing anywhere in the world or hereafter adopted or acquired, whether currently in use or not, all registrations and records thereof and all applications in connection therewith, whether pending or in preparation for filing, including registrations, recordings, and applications in any office or agency of the United States of America or any State thereof or any foreign country, all reissues, renewals, and extensions thereof, all of the goodwill of the business connected with the use of, and symbolized by such items, and all proceeds of, and rights associated with, the foregoing; (v) moral rights in those jurisdictions within where such rights are recognized, (vi) database protections in those jurisdictions that provide distinct legal protections for databases, (vii) all other intellectual property protections recognized within any of the jurisdictions, including but not limited to any applicable *sui generis* protections for intellectual property, and (viii) all proceeds of, and rights associated with, the foregoing (as appropriate to such rights), including the right to sue third parties for any actual or threatened past, present, or future infringements, dilutions or misappropriations of any of the foregoing, or for any injury to the goodwill associated with the use of any property or rights set forth in clause (iv), and all rights corresponding thereto throughout the world.

1.7 "**Licensed Software**" means the Material proprietary software product(s) indicated in the Order Form as Licensed Software under this Agreement.

1.8 "**M&S**" means the maintenance and support services provided by Material for the Licensed Software licensed under this Agreement.

1.9 "**Managed Service**" means the services provided by Material associated with the management of the Licensed Software on Licensee's behalf as further described in the Order Form.

1.10 "**Representatives**" means, as to any person, such person's affiliates and its or their directors, officers, employees, agents, and advisors (including, without limitation, financial advisors, counsel and accountants) bound by a written agreement or other legal obligation to maintain the confidentiality of the Confidential Information disclosed to them as required by the terms of Section 11.

1.11 "**Unit**" means the specific unit of measure identified in the Order Form applicable to Licensee's use of the Licensed Software.

2. License Grant.

2.1 License to Licensed Software. Subject to the terms and conditions of this Agreement, including but not limited to receipt of all applicable fees by Material, Material hereby grants to Licensee, and Licensee hereby accepts from Material, a limited, non-exclusive, non-transferable, non-assignable and non-sublicenseable license to use the Licensed Software, in a manner consistent with the limitations set forth in this Agreement, in connection with the Authorized Units during the Authorized Period.

2.2 Restrictions on Licenses. In addition to the restrictions set forth above, Licensee agrees that, except as otherwise expressly provided by this Agreement, it shall not: (a) exceed the scope of the licenses granted in this Section 2; (b) make copies of the Licensed Software; (c) sublicense, assign, delegate, rent, lease, sell, time-share or otherwise transfer the benefits of, use under, or rights to, the license granted in Section 2.1, and any attempt to make any such sublicense, assignment, delegation or other transfer by Licensee shall be void and of no effect; (d) reverse engineer, decompile, disassemble or otherwise attempt to learn the source code, structure or algorithms underlying the Licensed Software, except to the extent required to be permitted under applicable law; (e) modify, translate or create Derivative Works of the Licensed Software without the prior written consent of Material; (f) remove any copyright, trademark, patent or other proprietary notice that appears on the Licensed Software; or (g) combine or distribute any of the Licensed Software with any software that is licensed under terms that seek to require that any of the Licensed Software (or any associated Intellectual Property Rights) be provided in source code form (e.g., as "open source"), licensed to others to allow the creation or distribution of Derivative Works, or distributed without charge. The licenses provided by this Agreement are limited licenses, and Licensee acknowledges that this Agreement does not grant Licensee, and Material expressly disclaims the grant of, any license, immunity, or other right to or under any patent or other Intellectual Property Right of Material, whether directly or by implication, legal or equitable estoppel, exhaustion or otherwise, except for the limited licenses expressly set forth in Section 2.1. The restrictions in this Section 2.2 are not intended to prohibit Licensee from using third party managed services providers to manage the Licensed Software either at a Licensee's site or such third party's site solely on behalf and for the benefit of Licensee.

3. Orders. Licensee may place orders for additional Licensed Software, Authorized Units or to extend the Authorized Period with respect to the Licensed Software by specifying such order details in the order form agreed to in writing by the parties.

4. Ownership. The Licensed Software are licensed and not sold to Licensee. Material and its licensors own and retain all right, title and interest in the Licensed Software, any design changes, improvements, enhancements, Derivative Works, or modifications thereof or thereto, and any related and/or associated Intellectual Property Rights, whether developed by Material or by Licensee or its employees or independent contractors. Licensee shall cooperate with Material in good faith to the extent necessary for Material to arrange or obtain registration on behalf of Material of all Intellectual Property Rights in any design changes, improvements, enhancements, Derivative Works, or modifications to the Licensed Software. Notwithstanding anything to the contrary in this Agreement, Licensee acknowledges that it is not licensed under, and Material disclaims the grant of, any rights under Intellectual Property Rights of Material, whether by implication, exhaustion, estoppel, or under any other theory, other than those expressly specified in Section 2 above.

5. Services.

5.1 Licensed Software Maintenance and Support. Subject to the timely payment of the Fees for the applicable M&S fees as described in the Order Form, Material shall provide M&S for such Licensed Software as set forth in Exhibit A.

5.2 Managed Services. Subject to the timely payment of the Fees for the applicable Managed Services fee as described in the Order Form, Material shall provide Managed Services as set forth in the Order Form.

6. Payments.

6.1 Fees. Licensee shall pay to Material the applicable fees set forth in the Order Form in respect of the Licensed Software, M&S, Managed Services, and the other fees described in this Section 6 (collectively, the "**Fees**"). Licensee acknowledges that it shall have no right to return the Licensed Software, M&S, or Managed Services and that all Fees shall be non-refundable.

6.2 Payment Terms. All amounts payable to Material under this Agreement shall be paid in United States dollars and shall be due thirty (30) days from the date of invoice. Unless otherwise agreed by Material, all payments shall be made by wire transfer of immediately available funds to an account designated by Material, all wire transfer fees prepaid. Notwithstanding any other rights of Material, in the event of late payment by Licensee (other than a payment that is not made when due as a result of a bona fide dispute between the parties), Material shall be entitled to interest on the amount owing at a rate of 1% per month or the highest rate allowed by applicable law, whichever is less, compounded on a daily basis from the due date of payment until the date of actual payment.

6.3 Taxes; Set-offs. Any and all payments made by Licensee in accordance with this Agreement are exclusive of any taxes that might be assessed against Licensee by any jurisdiction. Licensee shall pay or reimburse Material for all value-added, sales, use, property and similar taxes; all customs duties, import fees, stamp duties, license fees and similar charges; and all other mandatory payments to government agencies of whatever kind, except taxes imposed on the net or gross income of Material. All amounts payable to Material under this Agreement shall be without set-off and without deduction of any taxes, levies, imposts, charges, withholdings and/or duties of any nature which may be levied or imposed, including without limitation, value added tax, customs duty and withholding tax.

7. Term. The term of this Agreement shall commence on the Effective Date and remain in effect until the end of the Authorized Period (the "**Term**"), unless this Agreement is terminated earlier in accordance with Section 8. The Authorized Period will renew automatically at the end of the applicable term, and the corresponding fees will become due, unless either party provides to the other advance written notice with respect to non-renewal at least thirty (30) days prior to the end of the then current term.

8. Termination.

8.1 Termination. This Agreement and the licenses granted hereunder may be terminated:

(a) by either party if the other has materially breached this Agreement, within thirty (30) calendar days after written notice of such breach to the other party if the breach is remediable or immediately upon notice if the breach is not remediable; or

(b) by Material upon written notice to Licensee if Licensee (i) has made or attempted to make any assignment for the benefit of its creditors or any compositions with creditors, (ii) has any action or proceedings under any bankruptcy or insolvency laws taken by or against it which have not been dismissed within sixty (60) days, (iii) has effected a compulsory or voluntary liquidation or dissolution, or (iv) has undergone the occurrence of any event analogous to any of the foregoing under the law of any jurisdiction.

8.2 Effect of Termination. Upon any expiration or termination of this Agreement, the license granted in Section 2 shall terminate immediately, and Licensee shall (i) immediately cease use of all Licensed Software, and (ii) return to Material all Licensed Software and other materials and information provided by Material and any copies thereof made by Licensee. Licensee shall certify to Material in writing that it has retained no copies of such Licensed Software, materials or information. Any termination or expiration shall not relieve Licensee of its obligation to pay all Fees accruing prior to termination. If the Agreement is terminated due to Licensee's breach, Licensee shall pay to Material all Fees set forth in the Order Form.

9. Warranty.

9.1 Material Warranty. The Licensed Software, when used by Licensee in accordance with the provisions of this Agreement, will perform, in all material respects, the functions described in the Order Form without any Errors (as such term is defined in Exhibit A) for a period of ninety (90) days from the date the Licensed Software was first delivered to Licensee (such period, the "**Warranty Period**").

9.2 Exclusive Remedies. Licensee shall report to Material, pursuant to the notice provision of this Agreement, any breach of the warranties set forth in this Section 9 during the relevant Warranty Period. In the event of a breach of warranty by Material under this Agreement, Licensee's sole and exclusive remedy, and Material's entire liability, shall be prompt correction of Errors or, if such correction is not possible, replacement of the Licensed Software in order to minimize any material adverse effect on Licensee's business.

9.3 Limitations of Warranties. No warranty or indemnification shall apply where the defect or error in the Licensed Software is caused by: (a) any use of the Licensed Software which is not in conformity with the provisions of this Agreement; (b) any repair, modification or installation of the Licensed Software not made or expressly authorized by Material; or (c) the use or attempted use of software other than the most current version supported by Material and made available to Licensee under the terms of this Agreement. Replacement or repair of a Licensed Software product shall not extend its warranty period beyond the original warranty expiration date.

9.4 Disclaimer of Warranty. Material does not represent or warrant that the operation of the Licensed Software (or any portion thereof) will be uninterrupted or error free, or that the Licensed Software (or any portion thereof) will operate in combination with other hardware, software, systems or data not provided by Material, except as expressly specified in the Order Form. Material does not provide assistance on the general use of the Licensed Software or problem diagnosis if Licensee is not current in its payment obligations. LICENSEE ACKNOWLEDGES THAT, EXCEPT AS EXPRESSLY SET FORTH IN SECTION 9.1, MATERIAL MAKES NO EXPRESS OR IMPLIED REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE LICENSED SOFTWARE OR SERVICES, OR THEIR CONDITION. MATERIAL IS FURNISHING THE WARRANTIES SET FORTH IN SECTION 9.1 IN LIEU OF, AND MATERIAL HEREBY EXPRESSLY EXCLUDES, ANY AND ALL OTHER EXPRESS OR IMPLIED REPRESENTATIONS OR WARRANTIES, WHETHER UNDER COMMON LAW, STATUTE OR OTHERWISE, INCLUDING WITHOUT LIMITATION ANY AND ALL WARRANTIES AS TO MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY OR NON-INFRINGEMENT OF THIRD-PARTY RIGHTS.

10. Limitation of Liability.

10.1 Exclusion of Consequential Damages. EXCEPT FOR A BREACH OF SECTION 11 BY EITHER PARTY, OR LICENSEE'S BREACH OF SECTION 2, IN NO EVENT SHALL MATERIAL OR

LICENSEE BE LIABLE IN AN ACTION UNDER TORT, CONTRACT, WARRANTY OR OTHERWISE FOR ANY: (a) SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE/EXEMPLARY DAMAGES OR LOSSES ARISING FROM OR RELATED TO A BREACH OF THIS AGREEMENT, THE OPERATION OR USE OF THE LICENSED SOFTWARE, OR THE SERVICES PERFORMED HEREUNDER, INCLUDING, WITHOUT LIMITATION, SUCH DAMAGES OR LOSSES ARISING FROM (i) LOSS OF BUSINESS, PROFIT OR REVENUES, (ii) LOSS OF DATA, PROGRAMMING OR CONTENT, (iii) FAILURE TO REALIZE SAVINGS OR OTHER BENEFITS, (iv) SUBSTITUTE PROCUREMENT, OR (v) DAMAGE TO EQUIPMENT, INCURRED BY EITHER PARTY OR ANY THIRD PARTY, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES OR IF SUCH DAMAGES OR LOSSES ARE FORESEEABLE; OR (b) DAMAGES OR LOSSES (REGARDLESS OF THEIR NATURE) FOR ANY DELAY OR FAILURE BY A PARTY TO PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT DUE TO ANY CAUSE BEYOND SUCH PARTY'S REASONABLE CONTROL**.**

10.2 Maximum Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, IN NO EVENT SHALL MATERIAL'S TOTAL LIABILITY TO LICENSEE FOR DAMAGES, LOSSES OR LIABILITY OF ANY KIND EXCEED, EITHER CUMULATIVELY OR IN THE AGGREGATE, THE FEES PAID BY LICENSEE TO MATERIAL UNDER THIS AGREEMENT.

10.3 Allocation of Risk. The parties acknowledge and agree that the limitations of liability in this Section 10 and in other provisions of this Agreement and the allocation of risk herein are an essential element of the bargain between the parties, without which neither party would have entered into this Agreement. Material's pricing and compensation under this Agreement reflects this allocation of risk and the limitation of liability specified herein. The parties further acknowledge and agree that the limitations of liability in this Section 10 shall apply even when a remedy available under breach of warranty or other similar provisions set forth under this Agreement has failed of its essential purpose.

11. Confidentiality. Unless otherwise agreed to in writing by the Disclosing Party, each Receiving Party agrees (a) to keep all Confidential Information in strict confidence and not to disclose or reveal any Confidential Information to any person (other than such Receiving Party's Representatives who (i) are actively and directly involved in providing or receiving products or services under this Agreement, and (ii) have a need to know the Confidential Information), and (b) not to use Confidential Information for any purpose other than in connection with fulfilling obligations or exercising rights under this Agreement. The Receiving Party shall treat all Confidential Information of the Disclosing Party by using the same degree of care, but no less than a reasonable degree of care, as it accords its own Confidential Information. The parties agree to cause their Representatives who receive Confidential Information to observe the requirements applicable to the Receiving Party pursuant to this Agreement with respect to such information, including, but not limited to, the restrictions on use and disclosure of such information contained in this Section 11. Notwithstanding the above, the obligations of the parties set forth herein shall not apply to any information that: was in the public domain at the time it was disclosed or has entered the public domain through no fault of the Receiving Party or any of its Representatives; was known to the Receiving Party free of any obligation of confidentiality before or after the time it was communicated to the Receiving Party by the Disclosing Party; is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information; is disclosed with the prior written approval of the Disclosing Party; is or becomes available to the Receiving Party on a non-confidential basis from a person other than the Disclosing Party or any of its Representatives who is not known by the Receiving Party to be otherwise bound by a confidentiality agreement with the Disclosing Party or any of its Representatives or to be under an obligation to the Disclosing Party or any of its Representatives not to transmit the information to the Receiving Party; or is disclosed pursuant to an order or requirement of a court, administrative agency or other governmental body; provided however, that the Receiving Party shall provide prompt written notice of such court order or requirement to the Disclosing Party to enable the Disclosing Party to seek a protective order or otherwise prevent or restrict such disclosure, and shall use reasonable efforts to cooperate with the Disclosing Party (at the Disclosing Party's expense) to obtain such protective order or other appropriate remedy. In the event that such protective order or other remedy is not obtained, or the Disclosing Party waives compliance in whole or in part, with the terms of this Agreement, the Receiving Party and its Representatives shall use reasonable efforts to disclose only that portion of the Confidential Information that is legally required to be disclosed or is the subject of such waiver, and to ensure that all Confidential Information that is so disclosed shall be accorded confidential treatment. Any materials or documents which have been furnished to the Receiving Party from the Disclosing Party shall be promptly returned or destroyed, at the option of the Disclosing Party, by the Receiving Party, within ten (10) days after (a) this Agreement has expired or has been terminated; or (b) a written notice is made by the Disclosing Party requesting such return or destruction. Upon such request, all copies, reproductions, compilations, summaries, analyses, or other documents containing or reflecting the Receiving Party's or its Representatives' use of the Confidential Information will be destroyed by the Receiving Party, and such destruction confirmed to the Disclosing Party in writing. The terms and obligations pertaining to confidentiality in this Agreement shall survive and remain in full force and effect for a period of five (5) years from the termination or expiration of this Agreement, unless the Disclosing Party expressly agrees in writing to release all or part of its Confidential Information from the restrictions imposed by this Agreement before such period has elapsed.

12. Indemnification.

12.1 By Material. Material will indemnify, defend and hold harmless Licensee and its employees (collectively, the "**Indemnified Parties**") from and against any and all losses arising from claims by a third party that the Licensed Software when used by Licensee as authorized in this Agreement (i) directly infringes a third party copyright or patent; or (ii) misappropriates, or unlawfully uses a third-party's trade secrets (collectively, "**Infringement Claims**"). Should any Licensed Software become, or in Material's opinion be likely to become, the subject of any Infringement Claim, then Licensee will permit Material, at Material's option and expense: to procure for Licensee the right to continue using the Licensed Software; to replace or modify the Licensed Software or portion thereof to be non-infringing; or to take any other action reasonably deemed advisable by Material related to such alleged infringement. In the event none of these remedies is available and/or practical, Material may, in its sole discretion, terminate the license and return to Licensee the license fees paid for the infringing licensed copies with respect to the then-current Authorized Period, reduced on a prorated basis for each month the Licensed Software is used during the Authorized Period.

12.2 Notice of Claim and Indemnity Procedure. In the event of a claim for which an Indemnified Party will seek indemnity or reimbursement under this Section 12, and as a condition of the indemnity benefits in Section 12, such party shall notify Material in writing as soon as practicable, but in no event later than thirty (30) days after receipt of such claim, together with such further information as is necessary for Material to evaluate such claim to the extent that the Indemnified Party is in possession or has knowledge of such information; provided that any delay in giving such notice shall not preclude the Indemnified Party(ies) from seeking indemnification or reimbursement thereunder if: (a) such delay has not materially prejudiced Material's ability to defend the claim; and (b) such delay does not materially affect the amount of any damages awarded for or paid in settlement of such claim. As a condition of the indemnity benefits in Section 12, Material shall have the right to assume full control of the defense of the claim, including retaining counsel of its own choosing. Upon the assumption by Material of the defense of a claim with counsel of its choosing, Material will not be liable for the fees and expenses of additional counsel retained by any Indemnified Party. The Indemnified Party(ies) shall cooperate with Material in the defense of any such claim.

12.3 Exclusions. Notwithstanding any other provision in this Agreement, Material shall have no obligation to indemnify or reimburse any Indemnified Party with respect to any Infringement Claim to the extent arising from (i) use of any Licensed Software in combination with any products or services other than those provided or approved by Material to Licensee under this Agreement; (ii) modification of the Licensed Software after delivery by Material to Licensee, except for such modifications performed by or expressly approved in writing by Material; (iii) use of any version of the Licensed Software other than the most current version made available by Material to Licensee hereunder; (iv) the failure of any Indemnified Party to use any Updates, corrections or enhancements to the Licensed Software that are made available by Material to Licensee hereunder; or (v) detailed, non-discretionary designs or specifications provided to Material by any Indemnified Party that necessarily caused such Infringement Claim. Licensee agrees to reimburse Material for any and all damages, losses, costs and expenses incurred as a result of any of the foregoing actions.

12.4 General Limitations. Notwithstanding the foregoing provisions, Material shall have no obligation to indemnify or reimburse for any losses, damages, costs, disbursements, expenses, settlement liability of a claim or other sums paid by any Indemnified Party voluntarily, and without Material’s prior written consent, to settle a claim. Subject to the maximum liability set forth in Section 10.2, the provisions of this Section 12 constitute the entire understanding of the parties regarding Material’s liability for Infringement Claims (including related claims for breach of warranty if any) and sole obligation to indemnify and reimburse any Indemnified Party.

13. Miscellaneous.

13.1 On-Site Precautions. Each party shall take all reasonable precautions to ensure the health and safety of the other party’s personnel while they are working at the other party’s premises. Each party shall indemnify the other in the event that any employee of the other party suffers personal injury or death as a result of the negligent act or omission of the first party.

13.2 Publicity. Licensee hereby grants Material the right to identify Licensee as a Material customer, and use Licensee’s name, mark, and/or logo on Material’s website and/or in Material’s marketing materials with respect to the same. In addition, Licensee agrees to participate in certain publicity activity, such as a case study or customer quote as may be described in the corresponding Order Form.

13.3 Notices. All notices, summons and communications related to this Agreement and sent by either party hereto to the other shall be written in English and sent by electronic mail with respect to Material to legal@material.security and with respect to Licensee to Licensee’s “Email for Notices” supplied below.

13.4 Assignment. Licensee shall not transfer or assign this Agreement or any of its rights or obligations hereunder, the Licensed Software or any component thereof, or any other materials provided hereunder, to any other person or entity, whether by written agreement, operation of law or otherwise, without the prior written consent of Material, which consent may be withheld for any reason whatsoever, as determined by Material in its sole discretion. Any purported assignment or transfer by Licensee without Material’s prior written consent shall be void and of no effect. Material may freely assign this Agreement, or delegate obligations under this Agreement, without the prior written consent of Licensee. Subject to the foregoing, any permitted assignment or transfer of or under this Agreement shall be binding upon, and inure to the benefit of, the successors, executors, heirs, representatives, administrators and assigns of the assigning or transferring party hereto.

13.5 Survival. Sections 1, 2.2, 4, 6, 8.2, 9.4, 10, 11, 13 shall survive the expiration or termination of this Agreement, or any default under or rejection in bankruptcy of this Agreement by Licensee.

13.6 Governing Law; Jurisdiction. This Agreement and all matters relating to this Agreement shall be construed in accordance with and controlled by the laws of the State of California, without reference to its conflict of law principles. The parties agree to submit to the non-exclusive jurisdiction and venue of the courts located in San Francisco, California and hereby waive any objections to the jurisdiction and venue of such courts.

13.7 No Agency; Independent Contractors. In connection with this Agreement each party is an independent contractor and as such will not have any authority to bind or commit the other. Furthermore, neither this Agreement, nor any terms and conditions contained herein, shall be construed as creating a partnership, joint venture or agency relationship or as granting a franchise.

13.8 Export Control; Compliance with Laws.

(a) **Export Control**. The Licensed Software and all other technical information delivered hereunder (collectively, "**Technical Data**") include technology and software and are subject to the export control laws and regulations of the United States ("**U.S.**"). Licensee agrees not to export, re-export or otherwise release any Licensed Software outside of the U.S. and to abide by such laws and regulations as to which Material may notify Licensee from time to time. Licensee further acknowledges and agrees that the Technical Data may also be subject to the export laws and regulations of the country in which the products are received, and that Licensee will abide by such laws and regulations.

(b) **Compliance with Laws**. Licensee shall comply with all applicable laws and regulations in its use of any Licensed Software, including without limitation the unlawful gathering or collecting, or assisting in the gathering or collecting of information in violation of any privacy laws or regulations. Licensee shall, at its own expense, defend, indemnify and hold harmless Material from and against any and all claims, losses, liabilities, damages, judgments, government or federal sanctions, costs and expenses (including attorneys' fees) incurred by Material arising from any claim or assertion by any third party of violation of privacy laws or regulations by Licensee or any of its agents, officers, directors or employees.

13.9 Force Majeure. Neither party shall be liable for failure to perform any of its obligations under this Agreement (except payment obligations) during any period in which such party cannot perform due to fire, earthquake, flood, any other natural disaster, epidemic, accident, explosion, casualty, strike, lockout, labor controversy, war, embargo, riot, civil disturbance, act of public enemy, act of nature, the intervention of any government authority, any failure or delay of any transportation, power, or for any other similar cause beyond either party's control. In the case of failure to perform, the failing party shall promptly notify the other party in writing of the reason for and the likely duration of the failure. The performance of the failing party's obligations shall be suspended during the period that the cause persists, and each party shall use commercially reasonable efforts to avoid the effect of that cause.

13.10 Severability and Waiver. To the extent that any term, condition or provision of this Agreement is held to be invalid, illegal or otherwise unenforceable under applicable law, then such term, condition or provision shall be deemed amended only to the extent necessary to render such term, condition or provision enforceable under applicable law, preserving to the fullest extent possible the intent and agreements of the parties set forth herein; in the event that such term, condition or provision cannot be so amended as to be enforceable under applicable law, then such term, condition or provision shall be deemed excluded from this Agreement and the other terms, conditions and provisions hereof shall remain in full force and effect as if such unenforceable term, condition or provision had not been included herein. The failure of a party to prosecute its rights with respect to a default or breach hereunder shall not constitute a waiver of the right to enforce its rights with respect to the same or any other breach.

13.11 Entire Agreement; Amendment. This Agreement, the Order Form, and any Exhibits referred to herein embody the entire understanding of the parties with respect to the subject matter hereof and shall supersede all previous communications, representations or understandings, either oral or written, between the parties relating to the subject matter hereof. It shall not be modified except by a written agreement signed on behalf of Licensee and Material by their respective duly authorized representatives. Licensee acknowledges that it is entering into this Agreement solely on the basis of the agreements and representations contained herein, and for its own purposes and not for the benefit of any third party. It is expressly agreed that the terms of this Agreement, the Order Form, and its Exhibits shall supersede the terms in any purchase order or other ordering document.

13.12 Exhibits. Each Exhibit to this Agreement shall be governed by the terms of this Agreement and the terms set forth therein. In the event of any inconsistency between the terms of this Agreement and the terms of the Exhibit, the terms of the Exhibit shall govern that Exhibit except as otherwise stated therein.

13.13 Headings. Captions and headings contained in this Agreement have been included for ease of reference and convenience and shall not be considered in interpreting or construing this Agreement.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed as of the Effective Date by their duly authorized representatives.

MATERIAL SECURITY INC.

By: ______________________________

Name:

Title:

Date:

LICENSEE

By: ______________________________

Name:

Title:

Date:

Email for Notices:

Exhibit A

Maintenance and Support for the Licensed Software

1. **Access to Material**. Material will provide Licensee with telephone and email support, Monday through Friday, from 8:00 a.m. to 6:00 p.m. Pacific Time (excluding US Federal holidays).

2. **Updates**. For so long as Licensee is timely in the performance of its obligations under this Agreement and these M&S terms, and has paid to Material the corresponding Fees, Material shall provide Licensee with access to Updates of the Licensed Software.

3. **Request for Problem Resolution.** All requests by Licensee for Error resolution will be logged after which Material will perform an initial diagnosis and determine as far as reasonably practical the source of any problem which may have led to the support request. All response and resolution times shall commence at the beginning of the next business day for requests for problem resolution that are logged during non-business hours.

4. **Bug Fixing.** Material will investigate incident reports concerning suspected problems with Licensed Software provided that (a) Licensee sends Material a written report, which includes evidence of the suspected Error, and (b) the incident can be reproduced or reasonably confirmed by Material. Material will use commercially reasonable efforts to promptly correct the Error or provide a workaround to permit Licensee to use the Licensed Software. Should an Error not be resolved quickly or for bugs that require further investigation, the procedures set forth in Section 5 of this exhibit shall apply.

5. **Escalation Procedures.** With regard to Errors submitted to Escalation Procedures, an action plan will be developed by the Material support team and communicated to Licensee. An Error will not be considered resolved until one of the following activities has been completed:

   (a) a resolution to the Error is obtained to Licensee's reasonable satisfaction;

   (b) a computer software code change in the form of a patch, workaround or a new revision that corrects the Error has been delivered to Licensee; or

   (c) an engineering commitment is made to correct the Error in a future release of the Licensed Software.

6. **Excluded Services.** Material shall not be obligated to fix any Error or problem:

   (a) where the Licensed Software is not used for its intended purpose; or

   (b) where the Licensed Software has been altered, damaged, modified or incorporated into other software in a manner not approved by Material; or

   (c) which is caused by Licensee's or a third party's software or equipment or by Licensee's negligence, abuse, misapplication, or use of the Licensed Software other than as specified in the Order Form.

7. **Installation of Updates and Delivery of Usage Logs**. Licensee acknowledges that periodic Updates and transfer of usage logs to Material are necessary to maintain optimal performance of the License Software. Licensee consents and hereby authorizes Material to install the Licensed Software, including any necessary third-party software, on Licensee's behalf as Licensee's agent. To facilitate the automatic installation of periodic Updates and the transfer of usage logs, the Licensed Software is

configured to allow for the automatic transfer of usage logs and installation of Updates. Licensee consents to Material's use of Licensee's usage logs for purposes of improving the features, functions and performance of the Licensed Software (including New Versions) and M&S.

8. **Term; Termination.** Subject to the terms and conditions set forth in this exhibit and the Agreement, and payment by Licensee of the corresponding Fees, M&S shall be provided to Licensee during the Authorized Period.

9. **Fees.** In consideration of Material's provision of M&S as set forth above, Licensee agrees to pay to Material the applicable fees set forth on the Order Form.

10. **End of Life Policy.** Licensee acknowledges that new features may be added to the Licensed Software based on market demand and technological innovation. Accordingly, as Material develops enhanced versions of the Licensed Software, Material may cease to maintain and support older versions. Material will use commercially reasonable efforts to notify Licensee of a Licensed Software undergoing the transition from supported to unsupported status at least six (6) months in advance of a Licensed Software's end of life ("**EOL**"). A time schedule for the termination of support will be provided on a product-by-product basis. After the six (6) month EOL notification period, Material will continue to offer Licensee the option of obtaining technical support at the then-current maintenance price for the discontinued product or version for a maximum period of one (1) year. Maintenance for discontinued products during a transitional support period shall include patches only for critical bug fixes and shall not include the addition of any new features, functionality, enhancements or improvements.

11. Definitions

11.1 "**Error**" means an incident that investigation reveals is caused by the Licensed Software's failure to perform materially in accordance with the specifications. An incident will not be classified as an Error if (a) the relevant Licensed Software is not used for its intended purpose; (b) the incident is caused by Licensee's or a third party's software or equipment (except to the extent Material has incorporated or packaged such third party's software or equipment in or with the Licensed Software); or (c) the version of the Licensed Software on which the Error has purportedly occurred is not the most current version of such Licensed Software made available to Licensee under this Agreement.

11.2 "**New Version**" means a release of a Licensed Software product or component thereof that implements a fundamental change in the software system philosophy and/or the software architecture, as determined by Material in its sole discretion, typically identified by a change in the digit to the left of the decimal point of the product numbering convention (x.x) (e.g., Product 3.0 to Product 4.0).

11.3 "**Update**" means a change to the current version of a Licensed Software product or a component thereof that does not constitute a New Version, as determined by Material in its sole discretion. An Update may include, without limitation, bug fixes, enhancements to the capability of an already partially supported feature or changes in the number, type, and/or specification of the supported platform(s), and is typically identified by a change in the digit to the right of the decimal point of the product numbering convention (x.x) (e.g., Product 3.1 to Product 3.2).

11.4 "**Upgrade**" means a migration by an existing licensee to a New Version.

Exhibit B

DATA PROCESSING AGREEMENT

This Data Processing Agreement made and entered into as of the above date (the “**Effective Date**”) consists of the terms and conditions set forth below, and in the Standard Contractual Clauses (as defined below) (the "**DPA**") that defines how Material Security, Inc. (“**Material Security**”) and the above party (“**Customer**”) agree to treat personal data (as defined below) that is contained in Customer Data.

This DPA forms part of the Agreement.

1. **Definitions.**

1.1. "**Agreement**" means, as applicable, the Material Security commercial agreement, or similar commercial agreement by and between Material Security and Customer with respect to Service.

1.2. "**Applicable Privacy Law**" means (i) prior to 25 May 2018, Applicable Privacy Law(s) 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data; and (ii) on and after 25 May 2018, 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) ("GDPR").

1.3. "**Customer Data**" means any data, information or other material provided, uploaded, or submitted by Customer to the Service in the course of using the Service.

1.4. "**Customer Personal Data**" means the personal data that is contained in Customer Data.

1.5. "**Data Exporter**" has the meaning given to it in the Standard Contractual Clauses.

1.6. "**Data importer**" has the meaning given to it in the Standard Contractual Clauses.

1.7. "**Data Subject**" has the meaning given to it in the Applicable Privacy Law.

1.8. "**European Economic Area**" or "**EEA**" means the Member States of the European Union together with Iceland, Norway and Liechtenstein.

1.9. "**Material Security Policy and Privacy Guidelines**" means the security standards attached to, and incorporated into, this DPA as Exhibit A.

1.10. "**Personal Data**" has the meaning given to it in the Applicable Privacy Law.

1.11. "**Processing**" has the meaning given to it in the Applicable Privacy Law, and "**process**" will be interpreted accordingly.

1.12. "**Service**" means the Material Security services received by Customer as set forth in the corresponding ordering document agreed to in writing by Material Security.

1.13. "**Standard Contractual Clauses**" means the Standard Contractual Clauses set out in Exhibit B.

1.14. "**Subprocessor**" has the meaning given to it in the Standard Contractual Clauses.

1.15. "**Subprocessor List**" means the list of subprocessors currently authorised by Material Security to process Customer Personal Data available at the following URL: https://material.security/subprocessors

2. **Scope and Application.** This DPA shall apply when Customer Personal Data is transferred to Material Security from any Customer or Customer's affiliates who are subject to the Applicable Privacy Law. In this context, Customer may act as "controller" and Material Security may act as

"processor" respectively with respect to the Customer Personal Data. Customer shall act as the "data exporter" and Material Security shall act as the "data importer" for the purposes of the Standard Contractual Clauses.

3. **<u>Data Processing</u>.**

3.1. **Instructions for Data Processing.** Material Security will process Customer Personal Data only in accordance with Customer's lawful instructions and in compliance with the Agreement, and will not process Customer Personal Data for any purpose other than to provide the Service. Processing outside of the scope of the Agreement will require the prior written agreement of the parties on the additional instructions for processing.

3.2. **Required Consents.** Where required by Applicable Privacy Law, Customer represents and warrants that it has obtained and/or will obtain all necessary consents and permissions required for the transfer of Customer Personal Data to, and processing of Customer Personal Data by, Material Security in accordance with the Agreement.

3.3. **Compliance with Laws.** Each party will comply with all applicable laws, rules, and regulations (including all applicable data protection law) in its performance of this DPA.

3.4. **Data Exports.** Customer represents and warrants that it has first obtained all necessary consents under Applicable Privacy Law with respect to the processing or transfer of Customer Personal Data originating from inside the EEA.

4. **<u>Security Responsibilities of Material Security</u>.**

4.1. **Security Measures**. Material Security shall implement and maintain appropriate technical and organizational security measures designed to protect and preserve the security, integrity and confidentiality of the Customer Personal Data described in the Material Security Policy and Privacy Guidelines.

4.2. **Material Security Personnel**. Material Security shall restrict access by Material Security personnel to Customer Personal Data (i) to only those personnel who need to access the Customer Personal Data in order to provide the Service; and (ii) as set out in the Material Security Policy and Privacy Guidelines.

4.3. **Records**. Material Security shall maintain relevant records with respect to Material Security's information security practices, and shall provide copies of such records as reasonably required by Customer to verify Material Security's compliance with this DPA.

4.4. **Audit by Customer**. Customer (or its third party independent auditors) may audit Material Security's compliance with the security measures set out in the Material Security Policy and Privacy Guidelines. Any such audit: (i) will be subject to Customer giving reasonable prior written notice to Material Security; (ii) will be performed at Customer's sole expense; and (iii) will be carried out by Customer in such a way as to mitigate any disruption to Material Security's business.

4.5. **Security Breach Notification**. If Material Security becomes aware of any unauthorised access to any Customer Personal Data stored on Material Security's equipment or in Material Security's facilities, then Material Security shall promptly notify Customer of such access and provide to Customer timely information and cooperation, as Customer may be required to address Customer’s reporting obligations under the Applicable Privacy Law. Any such notification shall not be construed as an acknowledgement by Material Security of any fault or liability with respect to the unauthorised access.

5. **Subprocessors.**

5.1. **Authorised Subprocessors**. Customer agrees that Material Security may use subprocessors to fulfil its obligations under the Agreement. The current subprocessor list Material Security published on the Material Security website at the following URL: https://material.security/subprocessors. Customer hereby consents to Material Security's use of subprocessors as described in this section 5. Before Material Security authorises any new subprocessor to process Customer Personal Data, Material Security will update the published subprocessor list or will otherwise notify Customer in writing of the identity of any new subprocessor. Customer may object in writing to the use of any new subprocessor within fifteen (15) days of the publishing of a new subprocessor list, provided that the written objection includes reasonable grounds for the objection. If Material Security elects to use any new subprocessor Customer previously objected to pursuant to this Section 5, Customer may terminate the Agreement by providing Material Security written notice of termination prior to the date Material Security begins to use such subprocessor.

5.2. **Subprocessor Obligations**. Where Material Security authorises a subprocessor to process Customer Personal Data as described in this section 5, Material Security will enter into a written agreement with each such subprocessor that contains provisions that are consistent to those contained in this DPA. Except as set forth in this DPA or as otherwise authorised in writing by Customer, Material Security will not permit any subprocessors to process Customer Personal Data.

6. **Cooperation.**

6.1. Material Security shall notify Customer of any requests received directly by Material Security from data subjects and shall provide to Customer such reasonable assistance as is required for Customer to comply with such data subject requests. Material Security shall only respond directly to such data subject requests on receiving Customer's written request and consent, provided that (to the extent permitted by Applicable Privacy Law) Customer shall be responsible for all reasonable costs arising from Material Security's provision of such assistance.

6.2. To the extent required under Article 28(3) GDPR, Material Security will assist Customer to comply with Articles 35 & 36 GDPR; in particular, Material Security will promptly notify Customer if it believes that its processing of Customer Personal Data is likely to result in a high risk to the privacy rights of data subjects, and upon reasonable request, will assist Customer to carry out data protection impact assessments and to consult where necessary with data protection authorities.

6.3. Following Customer’s request, Material Security shall destroy or return to Customer all Customer Personal Data in its possession. This requirement shall not apply to the extent that Material Security is required by any applicable law to retain some or all of the Customer Personal Data, in which case, Material Security shall use reasonable efforts to isolate and protect the Customer Personal Data from any further processing except to the extent required by such law.

7. **Limitation of Liability.** IN NO EVENT SHALL MATERIAL SECURITY BE LIABLE FOR ANY LOST DATA, LOST PROFITS, BUSINESS INTERRUPTION, REPLACEMENT SERVICE OR

OTHER SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR INDIRECT DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THEORY OF LIABILITY. MATERIAL SECURITY'S LIABILITY FOR ALL CLAIMS ARISING UNDER THIS DPA, WHETHER IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE AMOUNT OF FEES PAID OR PAYABLE BY CUSTOMER UNDER THE AGREEMENT DURING THE TWELVE (12) MONTH PERIOD PRECEEDING THE CLAIM.

8. **General.**

8.1. **Termination**. This DPA will terminate automatically upon termination of the Agreement.

8.2. **Conflict**. In the event of a conflict between the Agreement (other than this DPA) and this DPA, the terms of this DPA will take precedence to the extent of the conflict. In the event of a conflict between the Standard Contractual Clauses and the remaining terms of this DPA, the Standard Contractual Clauses will take precedence to the extent of the conflict. Nothing in this DPA modifies the Standard Contractual Clauses or affects any third party's rights under the Standard Contractual Clauses.

IN WITNESS WHEREOF, the parties hereto, by their duly authorized representatives, have executed and delivered this DPA as of the Effective Date.

MATERIAL SECURITY INC.

By: ______________________________

Name: ______________________________

Title: ______________________________

Date: ______________________________

CUSTOMER

By: ______________________________

Name: ______________________________

Title: ______________________________

Date: ______________________________

Email for Notices:

EXHIBIT A to the Data Processing Agreement

Material Security Policy and Privacy Guidelines

1. **SUBPROCESSORS.** Refer to subprocess list at the following URL: https://material.security/subprocessors

2. **TECHNICAL MEASURES.** Material Security's information security program includes safeguards that help protect your data as it is processed and stored by the service. Information about these safeguards is organized based on the following categories.

3. **AUTHENTICATION AND AUTHORIZATION.**

3.1. **Employee Account Assignment**. We assign individual named user accounts to employees who access Material Security's systems and devices. These assignments help us monitor and enforce accountability of employee activity.

3.2. **Employee-Level Privileges**. Our systems and devices enforce user roles or similar measures to control the extent of access we grant employees.

3.3. **Multi-Factor Authentication**. We enforce multi-factor authentication to better secure our computing resources from unauthorized logins.

4. **APPLICATION SECURITY**

4.1. **Secure Software Development**. We provide resources to Material Security developers to help identify and prevent common software vulnerabilities, including the OWASP Top 10. Developer code undergoes peer review prior to deployment, and internal security engineers review and analyze code for software components with higher potential security risk. More importantly, we prioritize building correct security libraries and primitives that help developers avoid writing vulnerable software in the first place.

4.2. **Web Application Security Review**. Third party security firms assess Material Security's web application at least annually. We address findings from this assessment according to the risk they pose to the security of the Material service. Material Security also maintains a Bug Bounty Program that invites the security research community to continuously test our security measures.

5. **NETWORK AND INFRASTRUCTURE SECURITY**

5.1. **Infrastructure Security Reviews**. We regularly perform vulnerability scans and third-party penetration tests on our infrastructure. We review and address findings from these activities to help maintain and improve our security posture.

5.2. **Configuration Standards**. We follow a rigorous security baseline configuration to maintain secure systems and infrastructure which includes removal of insecure default settings and minimal service exposure. These configurations are applied and enforced through code deployment requiring peer-review.

5.3. **Vulnerability And Patch Management**. To maintain awareness of potential security vulnerabilities, Material Security monitors public and private distribution lists, as well as reports submitted through our coordinated disclosure process. We prioritize patching of known vulnerabilities based on the severity of the issue and we deploy vendor-provided patches on a regular basis.

6. **ENCRYPTION**

6.1. **Secure Data Transmission**. All data is securely transferred between users and the Material Security system via TLS.

6.2. **Encryption Key Management And Security**. We leverage Google's Key Management Service to secure and store private keys throughout their lifecycle.

7. **DATA CENTER AND PHYSICAL SECURITY**

7.1. **Office Physical Security.** Material Security has one physical office located in Redwood City, California. Access to the Material Security office requires an authorized access badge. Only authorized individuals (e.g., employees and building management) are allowed to access the Material Security office. When an employee terminates employment, their key to the Material Security office is collected. Material Security also has security cameras in the office space, pointed at the door, recording all individuals' entry into and exit from the office.

7.2. **Data Center Security And Safeguards.** Material Security runs entirely on Google's Cloud Platform. Our physical controls are met by Google's compliance and regulatory requirements available here: https://cloud.google.com/security/compliance. Google is certified in a medley of requirements that include explicit physical security and environmental controls and these controls are inherited by our infrastructure.

8. **BUSINESS CONTINUITY AND OPERATIONAL RESILIENCE**

8.1. **Service Availability And Failover.** Since we run entirely on Google's Cloud Platform, we can leverage the massively scaled architecture implemented by Google to maintain high availability and, in the event of an outage, quickly failover to a separate availability zone on Google's Cloud Platform.

8.2. **Service Monitoring.** We monitor multiple internal and external reporting channels to detect service-related issues. On-call personnel are available 24x7x365 to confirm and respond to disruptions of the Material Security service.

8.3. **Communication And Reporting.** We update impacted customers using various communication methods depending on an incident's scope and severity.

9. **SECURITY INCIDENT MANAGEMENT**

9.1. **Incident Response Plan.** We maintain a formal incident response plan with established roles and responsibilities, communication protocols, and response procedures. We review and update this plan periodically to adapt it to evolving threats and risks to the Material Security service.

9.2. **Incident Response Team.** Representatives from key departments help address security-related incidents we discover. These personnel coordinate the investigation and resolution of incidents, as well as communication with external contacts as needed.

9.3. **Breach Notification.** Material Security will notify affected customers within 72 hours of validating an unauthorized disclosure of customer confidential information.

10. <u>LOGGING AND MONITORING</u>

10.1. **Log Analysis.** Material Security uses advanced tools to monitor and log traffic and detect and alert on suspicious activity which could potentially lead to security or performance incidents. The tools monitor in real time, but also log traffic and usage within the system, providing the ability to perform forensic research if necessary. Additionally, tools are configured to send notifications to administrators when an event requiring attention occurs.

10.2. **Change And Configuration Monitoring.** Material Security follows a defined development policy for making changes to the system used to support the services provided to their clients. The policy is designed to mitigate the risks of corrupted or destroyed information; degraded or disrupted computer performance; productivity loss; introduction of new vulnerabilities, configuration errors, and software bugs in infrastructure and code; and exposure to reputational risk. Material Security uses a software development platform to manage and record activities related to the change management process. The tool enforces version control and is used to document control points within the change management process. So that a structured change management process is followed, Material Security has created separate environments for development, staging, and production. The ability to implement changes into the production environment is limited to only those individuals who require it as part of their job function.

10.3. **Intrusion Detection.** We have a signature- and/or anomaly-based IDS/IPS in place, and sensors are in place at strategic points throughout the network. For production/GCP projects, we use GCP's built-in API/capabilities (Cloud Security Command Center & Event Threat Detection) which includes malicious content detection, anomaly detection as well as few additional categories of detection rulesets.

11. <u>CLOUD INFRASTRUCTURE SECURITY AND COMPLIANCE PROGRAM</u>

11.1. **Data Center And Physical Security.** Material relies on data center space under the control of the cloud infrastructure providers. These providers may have physical access to assets that contain data from Material Security services. As part of our third-party security review process, we confirm that these providers maintain appropriate physical security measures to protect their data center facilities.

11.2. **Business Continuity And Operational Resilience**. We deploy cloud-hosted products to infrastructure with multiple regions and zones. If failure of a service occurs within a single availability zone, Material Security will attempt to use cloud nodes in another zone.

11.3. **Encryption**. Material Security leverages in-transit and at-rest encryption to help secure data sent between Material Security, our customers, and the cloud infrastructure provider or to secure data that resides on cloud infrastructure. Because we use at-rest encryption features offered by infrastructure providers, those providers may also hold the private encryption keys. As part of our third-party security review process, we confirm that these providers maintain secure encryption key management processes.

Exhibit B to the Data Processing Agreement

Standard Contractual Clauses
(Controller-to-Processor Transfers)

This exhibit is attached to and forms part of the Material Security GDPR Data Processing Agreement (the "**DPA**") or other agreement between the customer identified therein (“**Customer**”) and Material Security governing the processing of Customer Personal Data (the “**Addendum**”) and the extent this Addendum is incorporated into by reference, and forms part of the agreement between the Customer and Material Security with respect to Material Security service (the “**Agreement**”) this Addendum shall apply to the same. Unless otherwise defined in this attachment, capitalised terms used in this attachment have the meanings given to them in the Addendum or Agreement.

SECTION I

Clause 1

Purpose And Scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex III.A. (hereinafter each “data exporter”), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex III.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter:“Clauses”).

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

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

Clause 2

Effect And Invariability of The Clauses

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

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

Clause 3

Third-Party Beneficiaries

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

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

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the Transfer(s)

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

Clause 7 - Optional

Not used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data Protection Safeguards

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

8.1 **Instructions**

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

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

8.2 **Purpose Limitation**

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

8.3 **Transparency**

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

8.4 **Accuracy**

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

8.5 **Duration Of Processing And Erasure Or Return Of Data**

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

8.6 **Security Of Processing**

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

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

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

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

8.7 **Sensitive Data**

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

8.8 **Onward Transfers**

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

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

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

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

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

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

8.9 **Documentation And Compliance**

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

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

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

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

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

Clause 9

Use Of Sub-Processors

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

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

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

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

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

Clause 10

Data Subject Rights

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

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

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

Clause 11

Redress

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

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

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

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

<u>SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES</u>

Clause 14

Local Laws And Practices Affecting Compliance With The Clause

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

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

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

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

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

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

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

Clause 15

Obligations Of The Data Importer In Case Of Access By Public Authorities

15.1 **Notification**

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

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

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

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

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

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

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

15.2 **Review Of Legality And Data Minimisation**

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

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-Compliance With The Clauses And Termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing Law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Grand Duchy of Luxembourg.

Clause 18

Choice Of Forum And Jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the district of Luxembourg City.

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

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

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The entity identified as “Customer” in the Addendum.

Address: The address for Customer specified in the Agreement.

Contact person’s name, position and contact details: The contact details associated with Customer’s account, or as otherwise specified in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities Information security data analysis and protection. Scanning for sensitive and suspicious indicators, security incident response, secure data warehousing, and any other processing required to provide the Services as set forth in the Agreement

Signature and date: By using the Material Security services to transfer Customer Personal Data to Third Countries, the data exporter will be deemed to have signed this Annex III.

Role (controller / processor): Controller

Data importer(s):

Name: " Material Security” as identified in the Addendum.

Address: The address for Material Security specified in the Agreement.

Contact person’s name, position and contact details: The contact details for Material Security specified in the Agreement.

Activities relevant to the data transferred under these Clauses:

Information security data analysis and protection. Scanning for sensitive and suspicious indicators, security incident response, secure data warehousing, and any other processing required to provide the Services as set forth in the Agreement

Signature and date: By transferring Customer Personal Data to Third Countries on Customer's instructions, the data importer will be deemed to have signed this Annex III.

Role (controller / processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of data subjects include corporate messaging data and associated office application data, including without limitation first and last names and email addresses.

Categories of personal data transferred

Corporate messaging data and associated office application data, including without limitation first and last names and email addresses. You can find more here: https://material.security/privacy

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Continuous basis as well as in accordance with Controller's instructions.

Nature of the processing

Data Processor will process Customer Personal Data subject to the Agreement and the Addendum for the purposes of providing the Services and related technical support in accordance with the Agreement and the Addendum and otherwise in accordance with any instructions of Controller.

Purpose(s) of the data transfer and further processing

Data Processor will transfer Customer Personal Data subject to the Agreement and the Addendum for the purposes of providing the Services and related technical support in accordance with the Agreement and the Addendum and otherwise in accordance with any instructions of Controller.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The applicable term of the Agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Corporate messaging data and associated office application data, including without limitation first and last names and email addresses on a continuous basis, for the purposes of providing the Services and related technical support in accordance with the Agreement and the Addendum for the applicable term of the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

<u>ANNEX II</u>

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons

The technical and organizational measures (including the certifications held by the data importer) as well as the scope and the extent of the assistance required to respond to data subjects' requests, are described in Exhibit B to the Data Processing Agreement.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

The technical and organisational measures that the data importer will impose on sub-processors are described in Exhibit B to the Data Processing Agreement.

<u>Exhibit C to the Data Processing Agreement</u>

SUPPLEMENTARY MEASURES

This Exhibit C forms part of the Data Protection Agreement and only applies to Material Security's Processing of Customer Personal Data that is subject to Exhibit B. All capitalized terms that are not expressly defined in this Exhibit C will have the meanings given to them in the Addendum or the Agreement. The following supplementary measures are intended to address the *Schrems II* decision.

Customer's Control Over Access to Data

The Material software is wholly deployed and contained within the customer's own Google Cloud Platform (GCP) project that is single-tenant and fully isolated from other customers. The customer's GCP project wholly contains the Material application and data. As a result, no customer data is ever stored or processed outside the project. All customer projects have GCP Security APIs enabled and monitored by Material's Security Team. The Material application does not store any customer data, including any personally identifiable information, anywhere outside of the customer's deployment. All systems that store or transmit customer data, including backup, are encrypted at rest (AES-256 or stronger). Only customer-designated operators can access the deployment for the purposes of administration and support.

Material Security's Policy Regarding

Government and Other Third-Party Requests for Customer Personal Data

Material Security is committed to providing users with control over their own data, to securing customer data against unauthorized access, and to protecting users' privacy. In accordance with this commitment, set out below is Material Security's policy for responding to third party requests, including requests by governmental entities, for Customer Personal Data:

1. Material Security will retain and, as appropriate, consult with expert legal counsel regarding all third-party requests for customer data.

2. Material Security will seek to refer each government request promptly to the relevant customer or user so that the customer or user can respond directly.

3. If the government declines to redirect its request to the relevant customer, Material Security will provide the customer with prompt notice of the request unless it is legally prohibited from doing so.

4. If Material Security is prohibited from providing prompt notice of a request to a customer, Material Security will provide such notice as soon as the prohibition expires or is no longer in effect.

5. Upon Customer's request and subject to reasonable confidentiality measures, Material Security will, to the extent legally permitted, provide a report to customer summarizing the number and types of government requests for customer data it has received in the applicable Report Period and how it has responded to them ("Transparency Report"). The Transparency Report for the most recent Report Period is set out below.

6. Material Security will assess the legality of all such requests and will comply with requests only if and to the extent it assesses that they are valid, lawful and compulsory.

7. Material Security will decline to comply with and undertake reasonable efforts to contest any request it determines is not absolutely required by applicable law, including any non-valid request under FISA 702, the CLOUD Act, or U.S. Executive Order 12333.

Material Security Transparency Report for 2021

Report Period: 1 January 2021 – 31 December 2021

Set out below is a summary of the government information requests, if any, Material Security has received for access to Customer Personal Data and how it has responded to them.

Government Information Requests:

- Material Security received 0 government requests of the type described in Paragraphs 150-202 of the judgment in the CJEU Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems,* nor is Material Security aware of any such orders in progress during the Report Period described above.

- During the Report Period no court has found Material Security to be eligible to receive process issued under FISA Section 702 and no such court action is pending.

- During the Report Period, Material Security has received 0 requests from U.S. or foreign governments under the CLOUD Act