

**SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA**



ITEM: 3.43
(ID # 27438)

MEETING DATE:
Tuesday, May 06, 2025

FROM : SHERIFF-CORONER-PA

SUBJECT: SHERIFF-CORONER-PA: Approve and Execute the License Agreement with Veritone, Inc. for Automated Redaction Software for Five (5) Years; All Districts [Total Cost \$940,000; Up to \$94,000 in Additional Compensation - 100% Sheriff's Budget]

RECOMMENDED MOTION: That the Board of Supervisors:

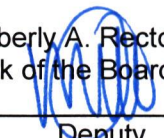
1. Approve the License Agreement with Veritone, Inc. for automated redaction software for five (5) years for a total aggregate amount of \$940,000 through March 31, 2030, and authorize the Chair of the Board to sign the License Agreement on behalf of the County; and
2. Authorize the Purchasing Agent, in accordance with Ordinance No. 459, based on the availability of fiscal funding and as approved to form by County Counsel to: (a) sign amendments that exercise the options of the License Agreement, including modifications of the statement of work that stay within the intent of the License Agreement, and (b) sign amendments to the compensation provisions that do not exceed ten percent (10%) or \$94,000 of the total cost of the Agreement.
3. Authorize the Purchasing Agent to issue Purchase Orders for the services provided not to exceed the approved amounts.

ACTION:Policy

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Washington, seconded by Supervisor Gutierrez and duly carried by unanimous vote, IT WAS ORDERED that the above matter is approved as recommended.

Ayes: Medina, Spiegel, Washington, Perez and Gutierrez
Nays: None
Absent: None
Date: May 6, 2025
xc: Sheriff

Kimberly A. Rector
Clerk of the Board
By: 
Deputy

**SUBMITTAL TO THE BOARD OF SUPERVISORS COUNTY OF RIVERSIDE,
STATE OF CALIFORNIA**

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	\$ 188,000	\$ 188,000	\$940,000	\$ 0
NET COUNTY COST	\$ 188,000	\$ 188,000	\$940,000	\$ 0
SOURCE OF FUNDS: 100% Sheriff's Budget			Budget Adjustment:	No
			For Fiscal Year:	25/26 – 29/30

C.E.O. RECOMMENDATION: Approve

BR: 25-065

BACKGROUND:

Summary

Riverside County Sheriff's Office (RSO) currently uses video, audio, and document redaction software to comply with the California Public Records Act (CPRA) and subpoena requests. Since the passing of Assembly Bills 748 and 1421 in 2019, all state and local agencies are mandated to make public records available for inspection to any person pursuant to the CPRA. The Assembly Bills, along with other State mandates, require agencies to produce records that include reports, forms, standalone audio, and video that require portions of the documents or media to be redacted prior to being released to the public. Important information pertaining to the investigation of crimes are redacted to protect the safety of the party or the successful completion of an investigation.

The automated redaction software offered by Veritone, Inc. is a cloud-based Artificial Intelligence (AI) head detection and transcription platform that easily redacts information from large quantities of audio and video media. The application will automatically redact any sensitive information such as individual human faces, key words, license plates, officer notepads, laptops, pattern-matched Personally Identifiable Information (PII), and sections of audio clips within audio and video-based evidence. Additionally, its application will locate words and/or phrases in automatically generated transcripts of interview room recordings, 911 calls, and audio from body cams or in-car video systems via keyword search. With the volume of requests RSO receives, having an application that will expedite the processing time and workflow will help the department meet CPRA request 10-day deadlines and minimize any civil penalties imposed on the County.

Impact on Residents and Businesses

Having an application that can automate the process of identifying and removing sensitive information from documents and digital files will enhance and offer increased efficiency, accuracy, and compliance with data privacy laws, while reducing the risk of human error. This tool will allow RSO's personnel to comply with CPRA and Subpoena required response times.

Additional Fiscal Information:

For the first ten (10) concurrent users, each license will cost \$16,000 annually, and any additional license thereafter will be discounted to \$14,000 each. The cost for twelve (12) licenses will total \$188,000 annually, and \$940,000 for the five (5) year License Agreement term.

RSO would like to request a ten (10) percent contingency in the amount of \$94,000 to account for new licenses added to the License Agreement. The 5-year cost with the 10% contingency request totals \$1,034,000, and all expenses will be paid from the Sheriff's Office budget.

**SUBMITTAL TO THE BOARD OF SUPERVISORS COUNTY OF RIVERSIDE,
STATE OF CALIFORNIA**

Contract History and Price Reasonableness

County Purchasing, on behalf of RSO, issued Request for Proposal (RFP) #SHARC-518 on February 10, 2024 seeking proposals from qualified bidders to provide multimedia redaction services. The solicitation was sent to 36 potential bidders and advertised publicly on the Purchasing website and PublicPurchase.com. Two (2) responses to the solicitation were received.

After careful evaluation and consideration of all aspects of the proposals and pre-award demonstrations by both bidders, the County evaluation committee, consisting of representatives from Sheriff's Information Services Bureau and Professional Standards Bureau, recommend the award to Veritone, Inc. as the lowest, most responsive, and highest scoring bidder.

ATTACHMENT A. Veritone License Agreement


Rebecca S Cortez, Principal Management Analyst 4/28/2025


Aaron Gettis, Chief of Deputy County Counsel 4/8/2025



LICENSE AGREEMENT

This License Agreement ("Agreement") is entered into as of the date of the last signature below ("Effective Date") by and between Veritone, Inc. (for itself and/or its subsidiaries), having a principal office located at 5291 California Avenue, Suite 350, Irvine, CA 92617 ("Veritone") and the entity listed under Licensee Information below ("Licensee"), with respect to license(s) to Veritone's aiWARE Platform and related Services.

LICENSEE INFORMATION				
Licensee Name:	Riverside County Sheriff's Office		Billing Contact Information	
Licensee Address:	1500 Castellano Rd., Jurupa Valley, CA 92509		Contact Name:	Kelly Wolfe
Contact Name:	Stephanie Mora Ponce		Contact Phone:	951-955-2458
Phone:	951-955-2043		Contact Email:	kwolfe@riversidesheriff.org
Email:	sponce@riversidesheriff.org		Email for Invoices:	
LICENSE AND SERVICES DETAILS				
Initial Term:	Start Date:	4/1/25	End Date:	3/31/2026
No. of Redact Concurrent Users:	Twelve (12) Redact Concurrent User		Yearly License Fee:	\$188,000
Services:	<ul style="list-style-type: none">- Veritone aiWARE™ Platform Access- Veritone Redact Application- Cognitive Processing (detailed below)- Standard webinar training and onboarding; standard technical support via email			
Cognitive Processing:	Redact License includes unlimited cognitive processing hours of media uploaded by Licensee through the Redact Application during the Term for twelve (12) Redact Concurrent Users. Additional Concurrent Redact Users can be purchased for an additional cost of \$14,000 per Redact Concurrent User per year to receive unlimited cognitive processing hours for each additional concurrent Redact user ("Additional Concurrent Redact Users").			
TERMS AND CONDITIONS				

- Master License Terms and Conditions.** This Agreement is governed by the Veritone Master License Terms and Conditions attached as Exhibit 1 and the Redact specific terms and conditions attached as Exhibit 2 as applicable (collectively, the "Terms and Conditions"), all of which are incorporated herein by reference. In the event of any conflict or inconsistency between the provisions of this Agreement and the provisions contained in the Terms and Conditions, the provisions of this Agreement shall govern and control. Capitalized terms used but not defined herein shall have the meanings ascribed to them in the Terms and Conditions. Veritone shall have the right to examine Licensee's User logs for the purpose of verifying the number of Concurrent Users, who have access to the Redact application.
- Redact Application and Cognitive Processing.** During the Term, Veritone will provide Licensee with access to the Redact Application and the cognitive processing specified above. Cognitive processing will be via an automated process within the Platform. Licensee will be responsible for uploading media in a format reasonably required by Veritone in order to ingest and process the media through the Redact Application. Licensee represents and warrants that it has the right to furnish to Veritone and to use such media in connection with Licensee's use of the Platform and Services.
- Limitations.** Licensee acknowledges that the Redact Application is intended to be used by Licensee only as a tool to support review and redaction of audio files and/or video footage, and the Redact Application and the results generated therefrom should not be considered or relied upon as a substitute for Licensee's customary review and redaction procedures. Licensee acknowledges that there are inherent limitations in artificial intelligence technologies,. Licensee is solely responsible for verifying all results generated by the Redact Application as part of its customary review and redaction procedures.
- Payment Terms.** Payment Terms will be set forth in the applicable Product Ts & Cs in Exhibit 2.
- Auto Renewal.** After the Initial Term (as defined in the table above), the term of this Agreement will automatically renew for additional one (1) year terms (each, a "Renewal Term" and together with the Initial Term, the "Term"), unless either Party provides the other written notice of non-renewal no later than 30 days prior to the expiration of the Initial Term or any Renewal Term
- Authority.** The person executing this Agreement on behalf of each party represents and warrants that he or she has full authority to execute the same on behalf of such party, and that no other actions or approvals are required for such party to enter into this Agreement and perform its obligations hereunder.

SIGNATURE BLOCK INCLUDED ON THE FOLLOWING PAGE

ACCEPTED AND AGREED BY:	
VERITONE, INC.	LICENSEE
Signed by: 	Signature: 
Signature: _____	Signature: _____
Name: Jon Gacek	Name: V. Manuel Perez
Title: GM Public Sector	Title: Chair, Board of Supervisors
Date: 3/13/2025	Date: 05/06/2025

DS



DS



ATTEST:
Kimberly Rector
Clerk of the Board

By: 
Deputy

APPROVED AS TO FORM:
Mihn C. Tran
County Counsel

By: 
Deputy County Counsel

**EXHIBIT 1
VERITONE, INC.
MASTER LICENSE TERMS AND CONDITIONS**

These Master License Terms and Conditions ("Terms and Conditions") apply to any License Agreement related to a license to access and use the Platform and associated Services (as such capitalized terms are defined hereinbelow) that references these Terms and Conditions.

1. License Agreement; Controlling Terms. For purposes hereof, "License Agreement" shall mean the written license agreement, order form, subscription form, statement of work or other written document that evidences the purchase by a licensee ("Licensee") of a license to access and use the Platform and Services from Veritone, Inc. or one of its subsidiaries (collectively, "Veritone"), either directly or through an authorized reseller of Veritone. The "Platform" means the Veritone aiWARE™ artificial intelligence (AI) operating system, the aiWARE suite of applications and other platforms and applications provided by Veritone, as applicable. The "Services" means the specific applications and services (such as AI processing, automated workflows, analytics, data storage and/or transfer, which among other capabilities, enables users to process, index, organize, manage, search, analyze and share audio, video and other data) made available to Licensee through the Platform, and any related configuration, installation, support and other services, whether deployed through Cloud Services or On-Premises Services, as defined herein. "Cloud Services" means any Services that are hosted by Veritone or third-party providers and made available to Licensee through the internet, as opposed to being available on Licensee's own computers. "On-Premises Services" means any Services that are hosted on a Licensee's own computers. The software components of the Platform and associated Services are referred to as "Software." The specific types and volumes of Services, fees and payment terms, number of authorized users (as applicable), and the term of the license shall be as set forth in the License Agreement. The License Agreement may also contain other license-specific terms and conditions. In the case of a License Agreement entered into directly between Veritone and Licensee, (a) the License Agreement and these Terms and Conditions are collectively referred to herein as this "Agreement"; (b) in the event of any conflict or inconsistency among the terms and conditions set forth in the License Agreement and in these Terms and Conditions, the rights and obligations of the parties shall be interpreted based on the following order of priority: (1) the License Agreement and (2) these Terms and Conditions; and (c) this Agreement constitutes the complete and exclusive agreement between Veritone and Licensee with respect to the Platform and Services, superseding and replacing any and all prior agreements, communications, and understandings, both written and oral, regarding such subject matter, and no additional or different provision contained in any purchase order form, order acknowledgment form, invoice or similar form of either party will be effective. In the case of a License Agreement entered into between Licensee and an authorized reseller of Veritone, these Terms and Conditions are referred to herein as this "Agreement" and represent the agreement between Veritone and Licensee governing the license(s) to the Platform and Services being purchased by Licensee from such reseller under that separate License Agreement, and Licensee acknowledges and agrees that Veritone is an intended third-party beneficiary of such License Agreement with respect to this Agreement and, therefore, may enforce its rights hereunder directly against Licensee.

1.1. Insurance

1.2. Without limiting or diminishing the CONTRACTOR'S obligation to indemnify or hold the COUNTY harmless, CONTRACTOR shall procure and maintain or cause to be maintained, at its sole cost and expense, the following insurance coverage's during the term of this Agreement. As respects to the insurance section only, the COUNTY herein refers to the County of Riverside, its Agencies, Districts, Special Districts, and Departments, their respective directors, officers, Board of Supervisors, employees, elected or appointed officials, agents, or representatives as Additional Insureds.

1.3. A. Workers' Compensation:

1.4. If the CONTRACTOR has employees as defined by the State of California, the CONTRACTOR shall maintain statutory Workers' Compensation Insurance (Coverage A) as prescribed by the laws of the State of California. Policy shall include Employers' Liability (Coverage B) including Occupational Disease with limits not less than \$1,000,000 per person per accident. The policy shall be endorsed to waive subrogation in favor of The County of Riverside.

1.5. B. Commercial General Liability:

1.6. Commercial General Liability insurance coverage, including but not limited to, premises liability, unmodified contractual liability, products and completed operations liability, personal and advertising injury, and cross liability coverage, covering claims which may arise from or out of CONTRACTOR'S performance of its obligations hereunder. Policy shall name the COUNTY as Additional Insured. Policy's limit of liability shall not be less than \$1,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this agreement or be no less than two (2) times the occurrence limit.

1.7. C. Vehicle Liability:

1.8. If vehicles or mobile equipment is used in the performance of the obligations under this Agreement, then CONTRACTOR shall maintain liability insurance for all owned, non-owned, or hired vehicles so used in an amount not less than \$1,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this agreement or be no less than two (2) times the occurrence limit. Policy shall name the COUNTY as Additional Insureds.

1.9. E. General Insurance Provisions - All lines:

1.10. Any insurance carrier providing insurance coverage hereunder shall be admitted to the State of California and have an A M BEST rating of not less than A: VIII (A:8) unless such requirements are waived, in writing, by the County Risk Manager. If the County's Risk Manager waives a requirement for a particular insurer such waiver is only valid for that specific insurer and only for one policy term.

1.11. The CONTRACTOR must declare its insurance self-insured retention for each coverage required herein. If any such self-insured retention exceeds \$500,000 per occurrence each such retention shall have the prior written consent of the County Risk Manager before the commencement of operations under this Agreement. Upon notification of self-insured retention unacceptable to the COUNTY, and at the election of the County's Risk Manager, CONTRACTOR'S carriers shall either; 1) reduce or eliminate such self-insured retention as respects this Agreement with the

COUNTY, or 2) procure a bond which guarantees payment of losses and related investigations, claims administration, and defense costs and expenses.

- 1.12. CONTRACTOR shall cause CONTRACTOR'S insurance carrier(s) to furnish the County of Riverside with either 1) a properly executed original Certificate(s) of Insurance and certified original copies of Endorsements effecting coverage as required herein, and 2) if requested to do so orally or in writing by the County Risk Manager, provide original Certified copies of policies including all Endorsements and all attachments thereto, showing such insurance is in full force and effect. Further, said Certificate(s) and policies of insurance shall contain the covenant of the insurance carrier(s) that thirty (30) days written notice shall be given to the County of Riverside prior to any material modification, cancellation, expiration or reduction in coverage of such insurance. In the event of a material modification, cancellation, expiration, or reduction in coverage, this Agreement shall terminate forthwith, unless the County of Riverside receives, prior to such effective date, another properly executed original Certificate of Insurance and original copies of endorsements or certified original policies, including all endorsements and attachments thereto evidencing coverage's set forth herein and the insurance required herein is in full force and effect. CONTRACTOR shall not commence operations until the COUNTY has been furnished original Certificate (s) of Insurance and certified original copies of endorsements and if requested, certified original policies of insurance including all endorsements and any and all other attachments as required in this Section. An individual authorized by the insurance carrier shall sign the original endorsements for each policy and the Certificate of Insurance.
- 1.13. It is understood and agreed to by the parties hereto that the CONTRACTOR'S insurance shall be construed as primary insurance, and the COUNTY'S insurance and/or deductibles and/or self-insured retention's or self-insured programs shall not be construed as contributory.
- 1.14. If, during the term of this Agreement or any extension thereof, there is a material change in the scope of services; or, there is a material change in the equipment to be used in the performance of the scope of work; or, the term of this Agreement, including any extensions thereof, exceeds five (5) years; the COUNTY reserves the right to adjust the types of insurance and the monetary limits of liability required under this Agreement, if in the County Risk Manager's reasonable judgment, the amount or type of insurance carried by the CONTRACTOR has become inadequate.
- 1.15. CONTRACTOR shall pass down the insurance obligations contained herein to all tiers of subcontractors working under this Agreement.
- 1.16. The insurance requirements contained in this Agreement may be met with a program(s) of self-insurance acceptable to the COUNTY.
- 1.17. CONTRACTOR agrees to notify COUNTY of any claim by a third party or any incident or event that may give rise to a claim arising from the performance of this Agreement.
- 1.18. General
- 1.19. CONTRACTOR shall not delegate or assign any interest in this Agreement, whether by operation of law or otherwise, without the prior written consent of COUNTY. Any attempt to delegate or assign any interest herein shall be deemed void and of no force or effect.
- 1.20. Any waiver by COUNTY of any breach of any one or more of the terms of this Agreement shall not be construed to be a waiver of any subsequent or other breach of the same or of any other term of this Agreement. Failure on the part of COUNTY to require exact, full, and complete compliance with any terms of this Agreement shall not be construed as in any manner changing the terms or preventing COUNTY from enforcement of the terms of this Agreement.
- 1.21. CONTRACTOR shall not provide partial delivery or shipment of services or products unless specifically stated in the Agreement.
- 1.22. CONTRACTOR shall not provide any services or products subject to any chattel mortgage or under a conditional sales contract or other agreement by which an interest is retained by a third party. The CONTRACTOR warrants that it has good title to all materials or products used by CONTRACTOR or provided to COUNTY pursuant to this Agreement, free from all liens, claims, or encumbrances.
- 1.23. Nothing in this Agreement shall prohibit the COUNTY from acquiring the same type or equivalent equipment, products, materials or services from other sources, when deemed by the COUNTY to be in its best interest. The COUNTY reserves the right to purchase more or less than the quantities specified in this Agreement.
- 1.24. The COUNTY agrees to cooperate with the CONTRACTOR in the CONTRACTOR's performance under this Agreement, including, if stated in the Agreement, providing the CONTRACTOR with reasonable facilities and timely access to COUNTY data, information, and personnel.
- 1.25. CONTRACTOR shall comply with all applicable Federal, State and local laws and regulations. CONTRACTOR will comply with all applicable COUNTY policies and procedures. In the event that there is a conflict between the various laws or regulations that may apply, the CONTRACTOR shall comply with the more restrictive law or regulation.
- 1.26. CONTRACTOR shall comply with all air pollution control, water pollution, safety and health ordinances, statutes, or regulations, which apply to performance under this Agreement.
- 1.27. CONTRACTOR shall comply with all requirements of the Occupational Safety and Health Administration (OSHA) standards and codes as set forth by the U.S. Department of Labor and the State of California (Cal/OSHA).
- 1.28. This Agreement shall be governed by the laws of the State of California. Any legal action related to the performance or interpretation of this Agreement shall be filed only in the Superior Court of the State of California located in Riverside, California, and the parties waive any provision of law providing for a change of venue to another location. In the event any provision in this Agreement is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions will nevertheless continue in full force without being impaired or invalidated in any way.

2. License, Reservation of Rights, Restrictions.

2.1. License.

- (a) **License of Platform and Cloud Services.** If Licensee entered into a License Agreement for Platform and Cloud Services, then Veritone hereby grants to Licensee, during the Term (as defined in Section 7), a nontransferable, nonsublicensable, nonexclusive, revocable license to access and use the Platform and Services, subject to the terms and conditions set forth in this Agreement, solely for Licensee's internal business purposes. For the avoidance of doubt, the Platform and Services and its content including Licensee Content, may not be displayed

publicly; provided that, subject to the provisions of Section 2.4 (Restrictions) and Section 11 (Indemnification) of this Agreement, Licensee may post, publish or otherwise share its owned or licensed content via the Platform for which sharing capabilities are enabled during the Term in accordance with the terms of this Agreement.

- (b) **License of Platform and On-Premises Services.** If Licensee entered into a License Agreement for Platform and On-Premises Services, then Veritone hereby grants to Licensee, during the Term (as defined in Section 7), a limited, nonexclusive, nontransferrable right and license to install the number of copies of the On-Premises Software in a production computing environment controlled by the Licensee, subject to the terms and conditions set forth in this Agreement, solely for Licensee's internal business purposes.

2.2. Reservation of Rights. The Platform and Services are licensed by Veritone to Licensee, and not sold. Licensee acquires only the right to use the Platform and Services in accordance with this Agreement and does not acquire any rights of ownership. Nothing herein shall be construed to transfer any rights, title or ownership of any Veritone or Veritone-licensed software, technology, materials, information or Intellectual Property Rights to Licensee. All right, title and interest (including all Intellectual Property Rights) in and to the Platform and Services shall at all times remain the sole and exclusive property of Veritone and/or its respective licensors and all use thereof shall inure to the benefit of Veritone and/or its respective licensors. Except as expressly set forth in this Agreement, no right or license, express or implied, is granted to Licensee or any third party by estoppel, implication, exhaustion or other doctrine of law, equity or otherwise with respect to any product, service, software, technology, materials, information or Intellectual Property Rights of Veritone or its affiliates or licensors. "Intellectual Property Rights" means all forms of proprietary rights, titles, interests, and ownership including patents, patent rights, copyrights, trademarks, trade dresses, trade secrets, know-how, mask works, *droit moral* (moral rights), publicity rights and all similar rights of every type that may exist now or in the future in any jurisdiction, including without limitation all applications and registrations therefore and rights to apply for any of the foregoing.

2.3. Third-Party Licenses. Certain software components of the Platform and Services are supplied pursuant to license agreements from third parties, and Licensee agrees that Licensee's use of the Platform and Services shall be subject to the provisions of such third-party license agreements.

2.4. Restrictions.

- (a) **License Restrictions.** Licensee agrees to use the Platform and Services only for lawful purposes and only as expressly authorized under this Agreement. Without limiting the generality of the foregoing, except as expressly authorized hereunder, Licensee agrees that it shall not, directly or indirectly: (i) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, display or otherwise make the Platform or Services, in whole or in part, including any content or data derived therefrom that is not directly owned by Licensee or for which Licensee has all necessary rights, available to any third party; (ii) reverse engineer, decompile, disassemble, modify, translate, reconstruct, omit, distort, obscure, copy or create derivative works of all or any portion of the Platform, Services, any underlying software, or any other Veritone Property (as defined below), or otherwise attempt to access the source code of the Platform or Services; (iii) incorporate any portion of the Platform or Services into Licensee's own programs or compile any portion of them in combination with Licensee's own programs; (iv) store or otherwise capture to physical media, or enable a third party to store or capture, the Platform or Services or any portion thereof; (v) permit any persons, other than Licensee's authorized users for which Licensee has procured User IDs (as defined in Section 3.1) pursuant to the License Agreement, to access and use the Platform or Services; (vi) permit any persons, other than Licensee's authorized personnel, and in the case of user-based Licenses, other than Licensee's authorized personnel for which Licensee has procured Licenses, to access and use the Services; (vii) defeat, circumvent or modify any authentication technology or other security measures, controls, limitations, or content or functionality filters contained in or associated with the Platform, Services or Software or otherwise attempt to access any aspect of the Platform or Services that Licensee has not been granted authorization to access under the License Agreement; (viii) remove any proprietary notices, labels or marks from the Software; (ix) violate any laws, rules or regulations in connection with its use of the Platform or Services, including any data or content, including Licensee Content contained in, transmitted through or derived therefrom (x) store or otherwise capture to physical media, or enable a third party to store or capture, the Platform or Services or any portion thereof.

- (b) **Prohibited Acts.** Licensee acknowledges and agrees that Licensee is prohibited from doing any act that may have the effect of undermining the integrity of the Platform, Services, any related computer systems, infrastructure or environment, or the methods by which Veritone provides Services to users. Without limiting the generality of the foregoing, Licensee agrees that it shall not, directly or indirectly: (i) defeat, circumvent or modify any authentication technology or other security measures, controls, limitations, or content or functionality filters contained in or associated with the Platform or Services, or otherwise attempt to access any aspect of the Platform or Services that Licensee has not been granted authorization to access under the License Agreement; (ii) deploy or facilitate the use or deployment of any script, routine, robot, spider, scraper or any other automated means, method or device with respect to Licensee's access and use of the Platform and Services for any purpose, including to access, view, select, or copy in whole or in part, any content, program, functionality of the Platform or Services, or any other proprietary information or trade secret of Veritone that is made available through the Platform or Services; (iii) deploy or facilitate the use or deployment of any program, system, means, method or device, for any purpose that places an unreasonable, unnecessary or excessive demand or load on the Platform, Services, or related hardware and connections, or prohibits, denies or delays access to Services by other users or otherwise threatens the continuous services of Veritone's ISPs, suppliers and vendors; (iv) introduce into the Platform or Services any program, executable file or routine (such as a worm, Trojan horse, cancel-bot, time bomb or virus) irrespective of whether any such program or routine results in detrimental harm to the Platform, Services, or any underlying systems or programs; (v) remove any proprietary notices, labels or marks from the Platform or Services; (vi) establish any direct or deep link or other connection to any specific page or location within the Platform or Services, other than the Platform log-in page; (vii) use or attempt to use another user's account without authorization, or interfere with another user's access to the Platform or Services; or (viii) access or use the Platform or Services to design, develop, build, market or support a competitive product or service. Licensee acknowledges and agrees that (a) the Software may contain certain software components that are supplied by third parties, including open source software, (b) such third-party software components are subject to the license terms imposed by such third parties, which may include restrictions and/or obligations related to the copying, modification, disclosure and/or distribution thereof, and (c) Licensee's use of such third-party software components shall be subject to such third-party license terms.

- (c) **Content and Data Restrictions.** Licensee agrees that it shall not: (i) upload or transmit through the Platform or Services any material, content, media or data ("Licensee Content") with respect to which Licensee does not either own all right, title and interest or have the appropriate license(s) for lawful use, or otherwise violate or infringe upon the intellectual property rights of any third party in Licensee's use of the Platform or Services, including the use or distribution of any data derived from the Platform or Services; or (ii) upload or transmit through the Platform or Services any Licensee Content: (1) which encourages conduct that would constitute a criminal offense, give rise to civil liability or otherwise violate any law; or (2) creates or attempts to create any liability of Veritone; or (3) for an unlawful purpose or in violation of any law.

3. Access and Use.

- 3.1. Access and Use of Platform and Cloud Services.** Veritone will enable Licensee to access and use the Platform for the duration of the Term, subject to any early termination of this Agreement in accordance with the terms hereof. Access to the Platform and Cloud Services will be through unique log-in credentials assigned to Licensee by Veritone (each, a "User ID"). Licensee shall be given that number of User IDs as specified in the License Agreement. Licensee will provide accurate and complete information in registering its authorized users for account access. Licensee acknowledges and agrees that the log-in credentials assigned hereunder are Confidential Information and may only be used by Licensee and its authorized users to access the Platform in accordance with the terms of this Agreement, and that Licensee will not publish, share, or otherwise enable any third party, directly or indirectly, to access the Platform for any purpose. Licensee further agrees that Licensee is responsible for its and its authorized users' use of the Platform, including use via the User IDs, and for any consequences thereof. Licensee agrees to immediately notify Veritone of any unauthorized or improper use of any log-in credentials of Licensee. All of the rights, obligations, restrictions, representations and warranties related to Licensee's access and use of the Platform under this Agreement shall apply to Licensee and all of Licensee's employees, contractors, consultants, representatives and agents (collectively, "Representatives"). Licensee shall be responsible for all acts and omissions of its Representatives in the performance of this Agreement and for any breach of this Agreement by any of its Representatives.
- 3.2. Delivery of Software; Availability of On-Premises Services; Installation and Use on Licensee Systems.** For On-Premises Services specified in the License Agreement, Veritone will deliver Software to Licensee or otherwise make the Software available for download by Licensee, as determined by Veritone, on or before the Start Date of the Term. Licensee will be solely responsible for the installation of the Software and for acquiring and maintaining all necessary hardware and/or third-party software required for the installation, implementation, and operation of the Software. Licensee will comply with any minimum hardware and/or software requirements, installation, configuration, operation, and maintenance requirements, instructions, recommendation and/or guidelines, that are communicated by Veritone in writing from time to time. Licensee acknowledges and agrees that, while Veritone may provide such requirements, instructions, recommendations and/or guidelines, the operation and performance of the Software within the Licensee-controlled environment will be impacted by a number of factors that are outside of Veritone's control, and accordingly, Veritone makes no representations, warranties or guarantees regarding the performance of the Software, Platform or Services in the Licensee-controlled environment, including but not limited to processing speeds, capacity, scalability or reliability.
- 3.3. Processing.** During the Term, Veritone will provide Licensee with access to the applications and cognitive processing specified in a License Agreement. Licensee is responsible for using media that is in a format supported by Veritone applications, in order to ensure that it is properly ingested and processed through such applications.

4. Intellectual Property.

- 4.1. Veritone Property.** As between Veritone and Licensee, Veritone and/or its respective licensors retain all right, title and interest (including Intellectual Property Rights) in and to the Platform and Services, including, but not limited to any elements, components, content, technology, software, code, documentation, derivative works, revisions, enhancements, modifications, condensations and/or compilations of or relating to the Platform and Services, and any trademarks, brand identifiers, materials and information, which are created, authored, developed, conceived and/or reduced to practice by Veritone and/or its respective licensors, including in connection with Veritone's provision of the Platform and Services to Licensee under this Agreement ("Veritone Property").
- 4.2. Licensee Property.** As between Licensee and Veritone, Licensee retains all right, title and interest (including Intellectual Property Rights) in and to the Licensee Content, and any software, technology, trademarks, brand identifiers, materials and information which are independently created, authored, developed, conceived or reduced to practice by Licensee.

5. Licensee Content.

- 5.1. Licensee Content Ownership.** Licensee represents and warrants that (i) Licensee and/or its licensors own all right, title and interest in and to all Licensee Content uploaded to or transmitted through the Platform or Services, or otherwise have all rights in such Licensee Content as necessary to furnish to Veritone and use the same in connection with Licensee's use of the Platform and Services and to grant the rights granted by Licensee in this Agreement, and (ii) such Licensee Content, and Licensee's and Veritone's use thereof as provided in this Agreement, do not and will not misappropriate or infringe upon any third party's Intellectual Property Rights, or violate any other rights of any third party.
- 5.2. License to Content.** In addition to any other rights expressly provided in the License Agreement, Licensee hereby grants to Veritone and its third-party service providers a non-exclusive, royalty-free, worldwide license to use and display all Licensee Content that Licensee provides to Veritone or that are otherwise uploaded to or captured by the Platform through Licensee's use of the Platform and Services, solely as required for Veritone to provide the Services and perform its obligations under this Agreement, directly or through its third party service providers, (ii) to share such Licensee Content with Veritone's third party service providers (and, where applicable, with Licensee's third party Representatives) in connection solely with Veritone's provision of the Platform and Services to Licensee, and (iii) to create aggregated or redacted forms of Licensee Content that do not identify Licensee or any of Licensee's users for Veritone's business purposes, including improvements and enhancements to the Platform and Services.
- 5.3. Data Security and Destruction.** Veritone shall keep all Licensee Content strictly confidential. Veritone shall maintain and use appropriate administrative, physical, and technical safeguards and measures for protection of the security, confidentiality and integrity of all Licensee Content uploaded to or transmitted through the Platform or Services, including protections against unauthorized disclosure or access, or accidental or

unlawful destruction, loss or alteration. Licensee Content shall be used and stored by Veritone solely to the extent required to provide the Services and perform its obligations under this Agreement, and Veritone shall not use or store the Licensee Content for any other purpose whatsoever. Veritone shall ensure that all personnel and third-party service providers having access to the Licensee Content are subject to confidentiality obligations with respect thereto. Veritone shall notify Licensee promptly in the event that Veritone determines that a security breach has resulted in an unauthorized disclosure of or access to Licensee Content. Upon termination of this Agreement or upon the written request of Licensee at any time, Veritone shall ensure the secure deletion and destruction of all Licensee Content.

- 5.4. Media and Metadata Hosting.** Unless otherwise expressly stated in the License Agreement, the media files and generated metadata associated with the Media Feeds as defined in the relevant License Agreement ("Stored Media") will be hosted in the Platform until the expiration of the Term or fifteen months following the initial ingestion and processing thereof, whichever occurs first.
- 5.5. Third Party Data Sources.** To the extent that any Licensee Content includes data from third party sources, or Licensee is otherwise granted access to data from third party sources through the Services, Licensee represents that it holds a valid and current license from such third party data sources to access and use such data (each, a "Data License"). Licensee acknowledges and agrees that certain analytics functionality offered as part of the Services will not be available to Licensee without Licensee's licensed right to access and use any and all such third party data. Licensee agrees to notify Veritone promptly upon the expiration or termination of any such Data License.
- 5.6. Data Protection Addendum.** In the case of U.S. personal information, the parties agree to be bound by the Data Protection Addendum attached as Exhibit 3. In the case of EU, UK or Switzerland personal information, Licensee shall contact Veritone for completion and execution of the applicable Data Protection Addendum.
- 6. Feedback.** During the Term, Licensee may provide Veritone with such written evaluations, comments and/or suggestions (collectively, "Feedback") regarding the Platform or Services. Licensee acknowledges and agrees that any Feedback provided to Veritone by Licensee hereunder shall be deemed to be Veritone Property and Licensee hereby assigns all right, title and interest in and to such Feedback to Veritone and acknowledges that Veritone will be entitled to, without limitation, implement and exploit any such Feedback in any manner without any restriction or obligation to Licensee. Notwithstanding the foregoing, Licensee acknowledges that Veritone is not obligated to act on any such Feedback.
- 7. Term and Termination.**
 - 7.1. Term.** The initial term of this Agreement and the License shall be as set forth in the License Agreement (the "Initial Term").
 - 7.2. Termination.** In addition to any termination rights expressly provided in the License Agreement, this Agreement may be terminated by either party if the other party (i) materially breaches any provision of this Agreement which remains uncured for a period of thirty (30) days from the date of written notice of such breach; or (ii) makes an assignment for the benefit of its creditors, is declared insolvent, or has a receiver or trustee in bankruptcy appointed to take charge of all or part of such party's property.
 - 7.3. Effect of Termination.** If at any time this Agreement is terminated, or upon expiration of the Term, (i) the License and all other rights granted to Licensee herein shall automatically terminate, (ii) Licensee shall immediately cease using the Platform and Services and shall comply with the Purge Obligation (defined below) with respect to the Platform, and (iii) Licensee shall no longer have access via the Platform to (x) any of the Licensee Content uploaded to the Platform by Licensee or (y) any of the content, data or analytics derived from any Licensee Content or Platform content that remains hosted on the Platform. As used herein, "Purge Obligation" means the complete deletion of all files on Licensee's computer systems, or other storage device or media under Licensee's ownership or control that contain copies of the Platform, or any portion thereof, including but not limited to, any data compiled by Licensee captured or otherwise obtained from or through the use of the Platform. Veritone shall have no liability to Licensee for any changes, limitations, suspensions, disablements, terminations or discontinuances of the Platform, or this Agreement.
 - 7.4. Survival.** The provisions of Sections 2.2 (Reservation of Rights), 4 (Intellectual Property), 5.3 (Data Security and Destruction), 6 (Feedback), 7.3 (Effect of Termination), 10.1 (Fees and Payments), 10.2 (Taxes), 12 (Confidentiality), 13 (Indemnification), 14.2 through 14.4 (Disclaimers), 15 (Limitation of Liability), and 16 (Miscellaneous) hereof, shall survive the expiration or any early termination of this Agreement for any reason.
- 8. Reporting Audit.** Except with respect to any License (or portion thereof) that includes unlimited processing, Licensee shall report all processing performed by the On-Premises Services. Licensee shall allow for automated transmission of usage logs from Licensee's data center to Veritone utilizing a transmission method and frequency reasonably specified by Veritone, unless a different reporting mechanism is approved in writing by Veritone. Veritone shall have the right, upon at least 15 days prior written notice to Licensee and at reasonable times, to examine Licensee's systems and records specifically pertaining to the usage of the On-Premises Software to verify Licensee's compliance with this Agreement. Upon Veritone's request, Licensee shall deliver to Veritone a written certification, signed by an authorized officer of Licensee, with respect to the accuracy of Licensee's usage reporting.
- 9. Removal of Software.** Upon expiration or termination of the license term specified in the License Agreement, Licensee shall immediately cease utilizing the On-Premises Services and, after first complying with any remaining reporting obligations pursuant to Section 8, Licensee shall remove from its systems and destroy any and all copies of the Software downloaded as part of the On-Premises Services (including all associated software components and all updates and modifications thereto) in its possession, and shall deliver to Veritone a written certification, signed by an officer of Licensee, with respect to Licensee's compliance with the foregoing obligation.

10. Fees, Charges and Payments.

10.1. Fees and Payments. In consideration for the License and Licensee's access and use of the Platform and Services, Licensee shall pay the license fees and any applicable additional fees as set forth in the License Agreement (collectively, the "Fees") pursuant to the payment terms set forth in the License Agreement. All Fees and other amounts due under this Agreement are payable in U.S. dollars.

10.2. Taxes. All Fees and any other amounts due hereunder are exclusive of taxes and similar assessments which may be imposed on the delivery of the Platform and Services and any other transactions contemplated hereby. Licensee shall be solely responsible for the payment of any and all sales, use, value added, excise, import, or other similar taxes or payments in lieu thereof, including interest and penalties thereon, imposed by any authority, government or governmental agency arising out of or in connection with amounts due hereunder (other than those levied on Veritone's income), and Licensee shall make such payments, and timely file any return or information required by treaty, law, rule or regulation. Upon request, Licensee shall provide Veritone with documentation evidencing such payments. If Veritone is required to pay any such taxes, duties or fees, Licensee shall reimburse Veritone immediately upon receipt of Veritone's invoice thereof.

10.3. Suspension of Platform Access. In addition to Veritone's termination rights set forth herein and without prejudice to any other rights of Veritone at law or in equity, Veritone may suspend its performance under this Agreement and any other agreement with Licensee and Licensee's access to the Platform if Licensee fails to comply with any part of its payment obligations set forth herein. Such suspension of service shall not suspend or otherwise affect Licensee's payment obligations set forth herein.

11. Changes. Veritone may, from time to time, in its sole discretion, make changes to the Platform and Services, or a portion thereof including, without limitation, formats, content, reports, functionality, and/or techniques.

12. Confidentiality.

12.1. The CONTRACTOR shall not use for personal gain or make other improper use of privileged or confidential information which is acquired in connection with this Agreement other than necessary in performance of Services. The term "privileged or confidential information" includes but is not limited to: unpublished or sensitive technological or scientific information; medical, personnel, or security records; anticipated material requirements or pricing/purchasing actions; COUNTY information or data which is not subject to public disclosure; COUNTY operational procedures; and knowledge of selection of contractors, subcontractors or suppliers in advance of official announcement.

12.2. The CONTRACTOR shall protect from unauthorized disclosure names and other identifying information concerning persons receiving services pursuant to this Agreement, except for general statistical information not identifying any person. The CONTRACTOR shall not use such information for any purpose other than carrying out the CONTRACTOR's obligations under this Agreement. The CONTRACTOR shall promptly transmit to the COUNTY all third party requests for disclosure of such information. The CONTRACTOR shall not disclose, except as otherwise specifically permitted by this Agreement or authorized in advance in writing by the COUNTY, any such information to anyone other than the COUNTY. For purposes of this paragraph, identity shall include, but not be limited to, name, identifying number, symbol, or other identifying particulars assigned to the individual, such as finger or voice print or a photograph.

12.3. Confidential Information. Each party (a receiving party) acknowledges and agrees that during the Term and in the course of using the Platform and Services and performing its duties under this Agreement, it may obtain information relating to the other party (a disclosing party), its and/or its customers', vendors', or third-party service providers' business or technologies, which is of a confidential and proprietary nature ("Confidential Information"). Such Confidential Information may include, but is not limited to, trade secrets, know-how, inventions, techniques, processes, software, algorithms, programs, schematics, data, technology roadmap, sales and marketing plans, and any other information which the receiving party knows or has reason to know is, or which by its nature would reasonably be considered to be, confidential, proprietary or trade secret information of the other party. Without limiting the foregoing, Confidential Information of Veritone shall include the Platform, Services and all associated software and documentation, as well as Feedback or any results of the evaluation or testing of the Platform or Services. The receiving party shall at all times, both during the Term and for a period of three (3) years after its termination (or, in the case of the Platform, Services and any associated software or trade secrets, in perpetuity), keep in trust and confidence all Confidential Information of the disclosing party, and shall not (i) use such Confidential Information other than as expressly authorized under this Agreement or as required for the receiving party to perform its obligations under this Agreement, or (ii) disclose any Confidential Information of the disclosing party to third parties (other than to Veritone's third-party service providers in connection with the performance of its obligations under this Agreement), without the disclosing party's prior written consent. The receiving party further agrees to immediately return to the disclosing party or destroy all Confidential Information (including all copies, extracts and summaries thereof) in the receiving party's possession, custody, or control upon the expiration or any termination of this Agreement. The obligations of confidentiality shall not apply to information which (a) has entered the public domain except where such entry is the result of the receiving party's breach of this Agreement; (b) prior to disclosure hereunder, was already in the receiving party's possession and not subject to any confidentiality obligations, as demonstrated by written evidence; (c) subsequent to disclosure hereunder is obtained by the receiving party on a non-confidential basis from a third party who has the right to disclose such information to the receiving party; or (d) has been independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information, as demonstrated by written evidence.

12.4. Permitted Disclosures. The receiving party may make disclosures (i) as required by applicable law or the rules of an stock exchange on which such party's shares are then traded; or (ii) as compelled by court order issued by a court of competent jurisdiction provided that the receiving party subject to such court order (a) provides the disclosing party with prompt written notice of any such compelled disclosure, (b) uses diligent reasonable efforts to limit disclosure, (c) uses commercially reasonable efforts to obtain confidential treatment or a protective order in connection with the information subject to such compelled disclosure, and (d) allows the disclosing party to participate in any such proceeding.

13. Indemnification.

- 13.1.** CONTRACTOR shall indemnify and hold harmless the County of Riverside, its Agencies, Districts, Special Districts and Departments, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives (individually and collectively hereinafter referred to as Indemnitees) from any liability, action, claim or damage whatsoever, based or asserted upon any services of CONTRACTOR, its officers, employees, subcontractors, agents or representatives arising out of this Agreement in any way relating to (i) property damage, bodily injury, or death; (ii) gross negligence or willful misconduct; or (iii) any condition outlined in Section 13.5 below. CONTRACTOR shall defend the Indemnitees at its sole expense including all costs and fees (including, but not limited, to attorney fees, cost of investigation, defense and settlements or awards) in any claim or action based upon such acts, omissions or services related to the instances outlined above.
- 13.2.** With respect to any action or claim subject to indemnification herein by CONTRACTOR, CONTRACTOR shall, at their sole cost, have the right to use counsel of their own choice and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of COUNTY; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes CONTRACTOR indemnification to Indemnitees as set forth herein.
- 13.3.** CONTRACTOR'S obligation hereunder shall be satisfied when CONTRACTOR has provided to COUNTY the appropriate form of dismissal relieving COUNTY from any liability for the action or claim involved.
- 13.4.** The specified insurance limits required in this Agreement shall in no way limit or circumscribe CONTRACTOR'S obligations to indemnify and hold harmless the Indemnitees herein from third party claims.
- 13.5. Veritone Indemnification of Licensee.** Veritone will defend, indemnify and hold harmless Licensee and its subsidiaries, affiliates, successors, assigns, licensors, and their respective members, officers, directors, employees, licensors, agents, from and against any liability or expense, including without limitation, any expenses, losses, damages, judgments, litigation costs and reasonable attorneys' fees that Licensee may incur as a result of any claim, suit or proceeding brought against Licensee by any third party arising or resulting from any allegation that the Platform or Services, or any part thereof, misappropriates or infringes upon any third party's Intellectual Property Rights, except to the extent such alleged or actual infringement arises from Licensee's negligence, misconduct or violation of any terms of this Agreement, including but not limited to: (1) Licensee's use of the Platform or Services outside the scope of rights granted to Licensee or otherwise in violation of this Agreement, (2) Licensee's use of the Platform or Services in combination with the products of third parties (other than those approved in writing by Veritone), or (3) modification of the Platform or Services not performed or provided by Veritone, if the infringement would not have occurred but for such modification. If the Platform or Services, in whole in part, become or, in Veritone's opinion are likely to become, the subject of an infringement claim or action, Veritone may, at its option: (x) procure, at no cost to Licensee, the right for Licensee to continue using the Platform or Services; (y) replace or modify the Platform or Services to render them non-infringing, provided there is no material loss of functionality; or (z) if, in Veritone's reasonable opinion, neither (x) nor (y) above is commercially feasible, terminate this Agreement and refund any prepaid amounts for unused Services during the terminated portion of the Term. The foregoing states Veritone's sole obligation and Licensee's exclusive remedy in the event any such infringement claim or action is commenced or is likely to be commenced.
- 13.6. Conditions.** The indemnifying party's indemnification obligations under this Section 13 are conditioned upon the indemnified party: (a) giving prompt notice of any such claim to the indemnifying party (except that any delay or failure to do so shall not relieve the indemnifying party of its obligations except to the extent the indemnifying party's ability to defend against such claims is materially prejudiced thereby); (b) granting sole control of the investigation, defense and settlement of each such claim or action to the indemnifying party (provided that the indemnifying party shall not settle any claim without the indemnified party's written approval unless such settlement includes an unconditional release of the indemnified party and does not impose any obligations on the indemnified party); and (c) providing reasonable cooperation to the indemnifying party and, at the indemnifying party's request and expense, assistance in the defense or settlement of the claim. The indemnified party shall have the right to participate in the defense of any claim with its own counsel at its own expense.

14. Warranties and Disclaimers.

- 14.1. Mutual Warranties.** Each party represents and warrants to the other that: (i) it is duly organized and validly existing under the laws of the jurisdiction of its incorporation or formation, and has full power, rights and authority to enter into this Agreement and carry out its obligations hereunder; (ii) the person executing this Agreement is authorized to do so on its behalf; (iii) this Agreement is valid and legally binding upon it; and (iv) the execution, delivery and performance thereof by such party does not conflict with any other agreement, instrument or understanding to which it is a party or by which it may be bound, nor would violate any applicable law or regulation.
- 14.2. DISCLAIMERS.** THE PLATFORM, SERVICES AND ANY OTHER VERITONE PRODUCTS AND SERVICES ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, VERITONE MAKES NO WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT TO THE PLATFORM AND SERVICES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY AS TO THE ACCURACY OF PROCESSING RESULTS, ANY WARRANTY OF MERCHANTABILITY, QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, WARRANTIES ARISING FROM COURSE OF DEALING OR USAGE OF TRADE, AND WARRANTIES OF NON-INFRINGEMENT. VERITONE DOES NOT WARRANT THAT THE PLATFORM AND SERVICES ARE ERROR-FREE, WILL RUN UNINTERRUPTED, OR THAT ALL ERRORS CAN OR WILL BE CORRECTED. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY LICENSEE FROM VERITONE SHALL CREATE ANY SUCH WARRANTY. LICENSEE HAS BEEN ADVISED AND AGREES THAT NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, VERITONE DOES NOT REPRESENT, WARRANT OR COVENANT THAT IT HAS SECURED ALL NECESSARY RIGHTS WITH RESPECT TO ANY PUBLIC MEDIA MONITORED AND/OR RECORDED BY THE PLATFORM AND IT IS LICENSEE'S SOLE RESPONSIBILITY TO IDENTIFY, SOLICIT AND OBTAIN ANY NECESSARY RIGHTS AND APPROVALS FOR ITS USE THEREOF.
- 14.3.** LICENSEE ACKNOWLEDGES AND AGREES THAT THE INTERNET IS A PUBLIC NETWORK OVER WHICH VERITONE EXERTS NO CONTROL. VERITONE MAKES NO REPRESENTATIONS OR WARRANTIES WHATSOEVER, AND SHALL HAVE NO LIABILITY WHATSOEVER, WITH RESPECT TO THE ACCURACY, DEPENDABILITY, PRIVACY, SECURITY, AUTHENTICITY OR COMPLETENESS OF DATA TRANSMITTED OVER OR OBTAINED USING THE INTERNET OUTSIDE OF THOSE SYSTEMS AND NETWORKS CONTROLLED BY VERITONE, OR ANY INTRUSION, VIRUS, DISRUPTION, LOSS OF COMMUNICATION, LOSS OR CORRUPTION OF DATA, OR OTHER ERROR OR EVENT CAUSED OR PERMITTED BY OR INTRODUCED THROUGH LICENSEE'S OWN USE OF THE INTERNET. LICENSEE IS SOLELY RESPONSIBLE FOR IMPLEMENTING ADEQUATE FIREWALL, PASSWORD AND OTHER SECURITY MEASURES TO PROTECT ITS SYSTEMS, DATA AND APPLICATIONS FROM UNWANTED INTRUSION, WHETHER OVER THE INTERNET OR BY OTHER MEANS.

15. LIMITATION OF LIABILITY.

- 15.1.** EXCEPT FOR (A) BREACHES OF EACH PARTY'S OBLIGATIONS UNDER SECTION 10 (CONFIDENTIALITY), AND (B) AMOUNTS FINALLY AWARDED OR SETTLED IN A THIRD PARTY CLAIM FOR WHICH A PARTY IS RESPONSIBLE UNDER SECTION 13 (INDEMNIFICATION), AND (C) LICENSEE'S PAYMENT OBLIGATIONS: (1) NEITHER PARTY, INCLUDING ITS OFFICERS, DIRECTORS, EMPLOYEES, REPRESENTATIVES AND AFFILIATES, SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, INCLUDING WITHOUT LIMITATION, LOST DATA OR LOST PROFITS, OR COSTS OF PROCURING SUBSTITUTE GOODS OR SERVICES, HOWEVER ARISING, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- 15.2.** EXCEPT WITH RESPECT TO VERITONE'S INDEMNIFICATION OBLIGATIONS HEREUNDER, VERITONE'S LIABILITY FOR DAMAGES ARISING OUT OF, RELATING TO OR IN ANY WAY CONNECTED WITH THIS AGREEMENT SHALL IN NO EVENT EXCEED THE FEES PAID BY LICENSEE TO VERITONE DURING THE TERM

16. Miscellaneous.

- 16.1. Force Majeure.** Except for the obligation to make payments of any Fees or any other amounts due hereunder, neither party will be liable for any failure or delay in its performance under the Agreement due to any cause beyond such party's control including acts of war, terrorism, acts of God, embargo, riot, sabotage, epidemic or pandemic, labor shortage or dispute, governmental act, or failure of the Internet, or any component comprising or operating the network infrastructure thereof (each, a "Force Majeure Event"), provided that the delayed party: (i) gives the other party prompt notice of such cause, and (ii) uses its reasonable commercial efforts to promptly correct such failure or delay in performance. If Veritone is unable to provide Service(s) for a period of sixty (60) consecutive days as a result of a continuing Force Majeure Event, either party may elect to terminate this Agreement.
- 16.2. Publicity.** Except as required or compelled by applicable law, the rules of any stock exchange, or a court order issued by a court of competent jurisdiction, neither party will make any public statement regarding, or disclose, advertise or publish the terms and conditions of this Agreement without the prior written consent of the other party; provided, however, that Veritone may reference Licensee on Veritone's website, other marketing materials, investor relations materials, and as a customer in Veritone's SEC filings.
- 16.3. Notices; Electronic Communications.** All notices to either party shall be in writing and delivered by hand, certified mail or overnight delivery service, or email to the addresses set forth in the License Agreement, or to such other address as either party shall provide by notice to the other party. Notices shall be deemed effective when delivered to the applicable address, unless any such notice is sent by email, in which event, notice shall be deemed effective upon confirmation of delivery by a "read receipt" or other such notice generated by the applicable email system, but in any event, by reply of the recipient of such notice. In connection with its use of the Platform and Services, Licensee consents to receiving communications from Veritone electronically. Veritone will communicate with Licensee by email or by posting notices on the Platform or through any Services. Licensee agrees that all notices, disclosures and other communications that Veritone provides to Licensee electronically satisfy any legal requirement that such communications be in writing.
- 16.4. General.** This Agreement shall be governed by and construed in accordance with the laws of the State of California (other than the conflict of law rules) and subject to the sole jurisdiction of the courts sitting in Orange County, California. Notwithstanding the foregoing, nothing herein shall be deemed to limit the parties' rights to seek injunctive relief in any other court of law of competent jurisdiction. This Agreement does not create any relationship other than Veritone as an independent contractor performing services covered by this Agreement and Licensee as the party contracting with Veritone for those services. No party is a partner or a legal representative of the other for any purpose whatsoever, nor is any party authorized to make any contract, agreement or warranty on behalf of any other party. Under no circumstance shall one party's employees be construed to be employees of the other party. Neither party may assign any of its rights or obligations under this Agreement without the prior written consent of the other party, except that either party may assign this Agreement in its entirety without the consent of the other party to an affiliate or to a successor entity in connection with any merger (by operation of law or otherwise), consolidation, reorganization, change in control, sale of all or substantially all of its assets related to this Agreement or similar transaction. This Agreement inures to the benefit of and shall be binding on the parties' permitted assignees, transferees and successors. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, the parties nevertheless agree that the court should endeavor to give effect to the parties' intentions as reflected in such provision, and the other provisions of this Agreement remain in full force and effect. The failure of either party to exercise or enforce any right or provision of this Agreement shall not constitute a waiver of such right or provision. This Agreement shall be fairly interpreted and construed in accordance with its terms and without strict interpretation or construction in favor of or against either party. Each party has had the opportunity to consult with counsel in the negotiation of this Agreement. Section headings are for reference purposes only, and should not be used in the interpretation hereof. No addendum, waiver, consent, modification, amendment or change of the terms of this Agreement shall bind either party unless in a writing that references this Agreement and is signed by duly authorized representatives of Licensee and Veritone. This Agreement may be executed in one or more counterparts (including fax or email) each of which shall be deemed an original but all of which taken together shall be deemed one and the same instrument.

EXHIBIT 2**REDACT TERMS & CONDITIONS**

- 1. Redact Application and Cognitive Processing.** During the Term, Veritone will provide Licensee with access to the Redact Application and the cognitive processing specified in the Agreement or order form. Cognitive processing will be via an automated process within the Platform. Licensee will be responsible for uploading media in a format reasonably required by Veritone in order to ingest and process the media through the Redact Application. Licensee represents and warrants that it has the right to furnish to Veritone and to use such media in connection with Licensee's use of the Platform and Services.
- 2. Limitations.** Licensee acknowledges that the Redact Application is intended to be used by Licensee only as a tool to support review

and redaction of audio files and/or video footage, and the Redact Application and the results generated therefrom should not be considered or relied upon as a substitute for Licensee's customary review and redaction procedures. Licensee acknowledges that there are inherent limitations in artificial intelligence technologies, and Veritone makes no representations or warranties as to the accuracy, quality, sufficiency or usefulness of the results generated by the Redact Application. Licensee is solely responsible for verifying all results generated by the Redact Application as part of its customary review and redaction procedures.

3. **Payment Terms.** The License Fee as set forth on page 1 of the License will be invoiced upon execution of this Agreement and will be due and payable upon receipt of the invoice. If applicable, Veritone will submit invoices on a monthly basis for the Additional Processing Fees Incurred during the previous month and such invoices will be due and payable by the first day of the month following the invoice date. Notwithstanding the foregoing, if the total Additional Processing Fees incurred during a calendar month are less than \$50.00, Veritone may, in its sole discretion, delay invoicing of such Additional Processing Fees until the total Additional Processing Fees incurred but not yet invoiced exceed \$50.00. All amounts are payable in U.S. dollars.

EXHIBIT 3

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") sets out the additional terms, requirements and conditions on which Company and/or its Affiliates will process Personal Data when providing Services to Customer under any agreement between Customer and Company and/or its affiliates. This DPA contains the mandatory clauses required by Article 28 (3) and the General Data Protection Regulation EU 2016/676.

This DPA includes the following Appendices, which are incorporated herein by reference (as applicable):

1. Appendix 1: Technical and Organizational Measures
2. Appendix 2: List of Authorized Subcontractors
3. Appendix 3: SCCs (if applicable)
4. Appendix 4: UK International Data Transfer Addendum (if applicable)

For the avoidance of doubt, the execution of any Agreement (as defined herein) shall be deemed to constitute acceptance of the Standard Contractual Clauses and acceptance of the list of Company Sub-processors that are incorporated herein, including any Appendices. Where the Customer wishes or is required to separately execute the Standard Contractual Clauses and accompanying appendices, the Customer should also complete the information as the data exporter and complete the information on the signature page and send the signed Standard Contractual Clauses to the Company by email to privacy@veritone.com.

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with the subject entity.

"Agreement" means any commercial agreement, including order forms, terms and conditions and this DPA, in each case as signed and executed by the Customer and the Company.

"Applicable Data Protection Laws" means all laws and regulations, including without limitation, laws and regulations of the European Union (e.g., the GDPR and any applicable legal regulations) and Switzerland, applicable to the Processing of Personal Data under the Agreement.

"Authorized Affiliate" means any of the Customer's Affiliate(s) which (a) is subject to applicable data protection laws and regulations, including those of the European Union, the European Economic Area and/or their Member States, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between the Customer and the Company, but has not signed its own order form or agreement with the Company.

"Company" means Veritone, Inc. or any of its subsidiary(ies) or affiliate(s) which is (are) a party to any Agreement, which shall include this DPA.

"Company Group" means the Company and its Affiliates engaged in the Processing of Personal Data.

"Control" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by European Union or Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or Member State law.

"Customer" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed the Agreement.

"Customer Data" means what is defined in the Agreement as customer data, provided that such data is electronic data and information submitted by or for the Customer pursuant to the Agreement. This DPA does not apply to Third-Party Services, including add-ons.

"Customer's Personal Data" means data Processed by the Company for the purposes of the Services provided in alignment with the Agreement, which is defined under Applicable Data Protection Laws as Personal Data. This includes, without limitation, (i) the names and/or contact information of individuals authorized by the Customer to access the Services (e.g., agents and supervisors); and (ii) information collected by the Customer when using the Services.

“Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.

“Effective Date” means the date of signing of this DPA by the Customer.

“GDPR” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“Personal Data” means any information relating to (i) an identified or identifiable natural person (the “Data Subject”) and (ii) an identified or identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, where for each (i) or (ii), such data is Customer Data.

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

“Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller, including as applicable any “service provider” as that term is defined by the GDPR.

“Services” means the services and other activities to be supplied to or carried out by the Company pursuant to the Agreement.

“Standard Contractual Clauses” or “SCCs” means the European Commission’s Standard Contractual Clauses for the transfer of Personal Data from the European Union to Processors (as set out in Annex to Commission Decision 2010/87/EU) established in third countries which do not ensure an adequate level of data protection.

“Sub-processor” means a processor appointed by the Company, on its behalf, to Process the Customer’s Personal Data excluding any employee of the Company, including without limitation, those processors set forth on **Appendix 2** annexed hereto.

“Supervisory Authority” means an independent public authority that is established by a Member State pursuant to Article 51 of the GDPR.

“Third-Party Services” means certain services and applications operated by various third parties available on or via the Services.

2. ROLE OF THE PARTIES AND THE PROCESSING ACTIVITIES

2.1 Roles of the parties. The parties acknowledge and agree that, with regard to the Processing of Personal Data, the Customer is exclusively acting as the Controller, the Company acts as the Processor and the Company will engage Sub-processors pursuant to the requirements set forth below.

2.2 Customer’s Processing of Personal Data. The Customer retains control of the Customer’s Personal Data and remains responsible for its compliance obligations under the Applicable Data Protection Laws, including providing any required notices, information and obtaining any required consents, and for the Processing instructions it gives to the Company. For the avoidance of doubt, the Customer’s instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws. The Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data. The Customer specifically acknowledges that its use of the Services will not violate the rights of any data subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the GDPR.

2.3 Company’s Processing of Personal Data. The Company shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with the Customer’s documented instructions.

2.4 Processing Instructions. The Company shall not Process the Customer’s Personal Data other than on the relevant Customer’s documented instructions unless the Processing is required by applicable laws to which the Company or the relevant Sub-processor is subject.

2.5 Additional Instructions. The Agreement and this DPA will be considered as the only documented instructions relevant to the purposes of this DPA. Any other instructions will be construed as additional instructions; provided, however, that the additional instructions are (a) reasonable instructions provided by the Customer; (b) approved and accepted by the Company; and (c) consistent with the terms of the Agreement. Any additional instructions shall be subject to an additional agreement that may entail additional pricing between the parties.

2.6 Customer Instructions. The Customer shall ensure that its instructions comply with all laws, regulations and rules applicable to the Customer Data and that the Company’s Processing of the Customer Data in accordance with the Customer’s instructions will not cause the Company to violate any applicable law, regulation or rule, including, without limitation, Applicable Data Protection Laws. The Company agrees not to access or use Customer Data, except as necessary to maintain or provide the Service, or as necessary to comply with a binding governmental order.

2.7 Compliance with applicable laws. Each party shall be in material compliance with applicable laws and regulations in the performance or receipt, as the case may be, of the Services hereunder, including but not limited to, Applicable Data Protection Laws.

3. AUTHORIZED SUBCONTRACTORS

3.1 Customer acknowledges and agrees that Company and its affiliates may: (1) engage third party subcontractors, agents, resellers, or auditors to access and Process Personal Data in connection with Services, (an current list of the Company's authorized Sub-processors is set forth on **Appendix 2**) and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation, the Processing of Personal Data (collectively, "Authorized Subcontractors").

3.2 At least thirty (30) days before enabling a new party in addition to Authorized Subcontractors to access or participate in the Processing of Personal Data, Company and/ or its affiliates will notify Customer of that update. Customer may reasonably object to such engagement in writing within thirty (30) days of receipt of notice by Customer. If Customer reasonably objects to an engagement in accordance with this Section 3.2, Company may provide Customer with a written description of commercially reasonable alternative(s), if any, to such engagement, including without limitation, modification to the Services.

3.3 If Customer does not object to the engagement of a third party in accordance with section 3.2, within thirty (30) days of notice by Company, such third party will be deemed an Authorized Subcontractor for the purposes of this DPA.

3.4 Company shall ensure that all Authorized Subcontractors (i) have executed confidentiality agreements that prevent them from disclosing any personal data both during and after their engagement by Company and (ii) are subject to obligations regarding the Processing of Personal Data that are no less protective than those set out in this DPA.

4. DATA SUBJECT REQUESTS

4.1 Data Subject Requests. The Company shall, to the extent legally permitted, promptly notify the Customer if the Company receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure (the "right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request."

4.2 Cooperation with Customers on Requests. The Customer must provide Data Subjects with a contact or means deemed adequate to exercise their rights with the Customer. In any case, the Company shall not be required to reply directly to the Data Subjects Request or provide a direct helpline or any other communication challenge for purposes of responding to a Data Subject Request.

4.3 Request Assistance. To the extent the Customer, in its use of the Services, does not have the ability to address a Data Subject Request, the Company shall upon the Customer's request provide commercially reasonable efforts to assist the Customer in responding to such Data Subject Request, to the extent the Company is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Laws. To the extent legally permitted, the Customer shall be responsible for any costs arising from the Company's provision of such assistance.

4.4 The Company must take such technical and organizational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

- (a) the rights of Data Subjects under the Applicable Data Protection Laws, including subject access rights, the rights to rectify and erase Personal Data, object to the Processing and automated Processing of Personal Data, and restrict the processing of Personal Data; and
- (b) information or assessment notices served on the Customer by any supervisory authority under the Applicable Data Protection Laws.

4.5 The Company must notify the Customer immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Applicable Data Protection Laws. The Company must notify the Customer without undue delay if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Applicable Data Protection Laws. The Company will give the Customer its full cooperation and assistance in responding to any complaint, notice, communication or Data Subject Request. The Company must not disclose the Personal Data to any Data Subject or to a third party other than at the Customer's request or instruction, as provided for in this DPA or as required by law.

5. CROSS BORDER TRANSFER OF PERSONAL DATA - IF APPLICABLE

5.1 Any transfer of Personal Data from member states of the European Union, Iceland, Liechtenstein, Norway, Switzerland or the United Kingdom (the "EEA") to any countries which do not ensure an adequate level of data protection within the meaning of the laws and regulations of these countries shall, to the extent such transfer is subject to such laws and regulations, be undertaken by Company through the Standard Contractual Clauses provided in Appendix 3 of this Addendum and the UK International Data Transfer Agreement.

5.2 Where Customer consent is granted, the Company may only Process, or permit the Processing, of Personal Data outside the EEA under the following conditions:

- (a) The Company is Processing Personal Data in a territory which is subject to a current finding by the European Commission under the Applicable Data Protection Laws that the territory provides adequate protection for the privacy rights of individuals.
- (b) The Company participates in a valid cross-border transfer mechanism under the Applicable Data Protection Laws, so that the Company and, where appropriate, the Customer, can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the GDPR.

5.3 If any Personal Data transfer between the Customer and the Company requires execution of SCC in order to comply with the Applicable Data Protection Laws (where the Customer is the entity exporting Personal Data to the Company outside the EEA), the parties will complete all relevant details in, and execute, the SCC contained in **Appendix 3** and take all other actions required to legitimize the transfer.

5.4 If the Customer consents to appointment by the Company located within the EEA of a subcontractor located outside the EEA, then the Customer authorizes the Company to enter into the SCC contained in **Appendix 3** with the subcontractor in the Customer's name and on its behalf. The Company will make the executed SCC available to the Customer upon request.

6. CONFIDENTIALITY

6.1 Confidentiality. The Company shall ensure that all of its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. The Company shall ensure that such confidentiality obligations survive the termination of the personnel engagement. The Company shall bear responsibility for any breach of confidentiality obligations by any personnel engaged in the Processing of Personal Data as if such breach was the act of the Company itself.

6.2 Limitation of Access. The Company shall ensure that the Company's access to Personal Data is limited to those of its personnel performing Services in accordance with the Agreement.

7. SECURITY

7.1 Protection of Customer Data. Taking into account the state of the art and the costs of implementation, the Company shall maintain appropriate technical and organizational measures for the protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, all as set forth more fully on **Appendix 1** annexed hereto.

7.2 Customer Responsibilities. The Customer acknowledges that the Services includes certain features and functionalities that the Customer may elect to use that impact the security of the data Processed by the Customer's use of the Services. The Customer is responsible for reviewing the information the Company makes available regarding its data security, including its audit reports, and making an independent determination as to whether the Services meets the Customer's requirements and legal obligations, including its obligations under this DPA. The Customer is further responsible for properly configuring the Services and using available features and functionalities to maintain appropriate security considering the nature of the data Processed by the Customer's use of the Services.

7.3 Notification of Data Breach. The Company shall, to the extent permitted by law, notify the Customer within 48 hours after becoming aware of any Data Breach. To the extent such Data Breach is caused by a violation of the requirements of this DPA by the Company, or by the Company's negligence or wilful misconduct, the Company shall use best efforts to identify and remediate the cause of such Data Breach to the extent the remediation is within the Company's reasonable control. The obligations herein shall not apply to incidents that are caused by the Customer or the Customer's authorised users.

8. AUDITS

8.1 Upon the Customer's written request at reasonable intervals and no more than once a year, and subject to reasonable confidentiality controls, the Company shall make available to the Customer (or the Customer's independent, third-party auditor), which is not a competitor of the Company, information regarding the Company's compliance with the obligations set forth in this DPA. The Customer may contact the Company in accordance with the "Notices" section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. The Customer shall reimburse the Company for any time expended for any such on-site audit at the Company's then-current professional services rate, which shall be made available to the Customer upon written request. Prior to the commencement of any such on-site audit, the Company and the Customer shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which the Customer shall be responsible.

8.2 The Customer shall promptly notify the Company with information regarding any non-compliance discovered during the course of an audit. For the avoidance of doubt, any information obtained by the Customer under this Section 8 shall be treated as Confidential Information of the Company in accordance with the Agreement.

9 EUROPEAN ECONOMIC AREA SPECIFIC PROVISIONS

9.1 GDPR and UK-GDPR. The Company will Process Personal Data in accordance with the GDPR requirements directly applicable to the Company's provision of its Services as Processor.

9.2 Data Protection Impact Assessment. Upon the Customer's request, the Company shall provide reasonable assistance (at the Customer's expense) needed to fulfill the Customer's obligation under the GDPR to carry out a data protection impact assessment to the Customer's use of the Services, to the extent the Customer does not otherwise have access to the relevant information, and to the extent such information is available to the Company. The Company shall provide reasonable assistance to the Customer in connection with Customer's cooperation or prior consultations with any Supervisory Authority or other competent data privacy authorities, which the Customer reasonably considers to be required by articles 35 or 36 of the GDPR.

10 AUSTRALIAN AREA SPECIFIC PROVISIONS

When applicable, the Company will process Personal Data in accordance with the Australian Privacy Act 1988 requirements directly applicable to the Company's provision of Services as Processor.

11 DELETION OR RETURN OF CUSTOMER DATA

11.1 At the Customer's request, the Company will promptly give the Customer a copy of or access to all or part of the Customer Data or Customer's Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of any Agreement for any reason or expiry of its term, the Company will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any Customer Data or Customer's Personal Data related to such Agreement in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires the Company to retain any documents or materials that the Company would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

11.4 The Company will certify in writing that it has destroyed the Customer Data or Customer's Personal Data within 30 days after it completes the destruction.

11.5 Deletion. Following termination or expiry of any Agreement, the Company will delete all Customer Data or Customer's Personal Data within the timeframe stated in the Agreement. In case of any dispute, the Customer Data or Customer's Personal Data may be maintained by the Company upon the Customer's 30 days' prior written notice, at the Customer's sole expense.

11.6 Return. In the event the Customer requests the return of Customer Data or Customer's Personal Data, the Company will provide timely assistance to provide the return of such Customer Data or Customer's Personal Data, at the Customer's sole expense.

12. AUTHORIZED AFFILIATES

12.1 Contractual Relationship. The parties acknowledge and agree that, by executing the Agreement, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between the Company and each such Authorized Affiliate subject to the provisions of the Agreement. Each Authorized Affiliate expressly agrees to be entirely bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by the Customer.

12.2 Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communications with the Company under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

12.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with the Company, it shall, to the extent required under Applicable Data Protection Laws, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

(a) Except where Applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against the Company directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together.

(b) The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an onsite audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on the Company

and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

13. LIMITATION OF LIABILITY

13.1 Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and the Company, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs taken together.

13.2 For the avoidance of doubt, the Company's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by the Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to the Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

This DPA supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this DPA, including any prior data processing addenda entered into between the Company and the Customer. If there is any conflict between this DPA and any agreement, including the Agreement, the terms of this DPA shall control.

Contact for data protection enquiries: privacy@veritone.com

APPENDIX 1

TECHNICAL AND ORGANISATIONAL MEASURES

In order to protect the confidentiality, integrity and availability of its internal and Customer Data, the Company has implemented an information security program that includes the following technical, administrative/organizational, and physical controls:

1. Governance and Organizational Controls

Reporting relationships, organizational structures and proper assignment of responsibilities for systems controls, including the appointment at the executive level of a Chief Information Officer of the Company has implemented a risk assessment framework used to evaluate risks throughout the Company on an ongoing basis. The risk management process incorporates managements' risk tolerance, and evaluations of new or evolving risks. The Company implements various technical and organizational measures designed to ensure a level of security appropriate to the risks posed to customer data. Such measures seek to prevent unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of access to customer data. Consistent with industry standards set forth in applicable data protection laws, such measures include:

1.1 Information Security Program

The Company maintains a formal information security program containing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. This program is reasonably designed to (i) safeguard the security and confidentiality of customer information, (ii) protect against anticipated threats or hazards to the security or integrity of the information, and (iii) protect against unauthorized access to or use of the information. This is accomplished by:

- ✓ Written security policies designed to be consistent with the ISO/IEC 27001:2013 information security standards, including IT Security Policies and an Acceptable Use agreement;
- ✓ Written privacy policies;
- ✓ New Hire and Annual security awareness training for staff; and
- ✓ Incident Response and Disaster Recovery plans;

1.2 Access Control of Processing Areas

The Company implements suitable measures to prevent unauthorized persons from gaining access to the data processing equipment (namely database and application servers and related hardware) where customer data is accessed, processed or used. This is accomplished by:

- ✓ establishing security areas;
- ✓ securing data processing equipment and personal computers;
- ✓ establishing access authorizations for employees and third parties, including the respective documentation;
- ✓ restriction of access card-keys;
- ✓ all access to the data center where personal data are hosted is logged, monitored, and tracked; and
- ✓ the data center where personal data are hosted is secured by appropriate security measures.

2. Access Control to Data Processing Systems

The Company implements suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished by:

- ✓ identification of the individual user to the Company systems;
- ✓ automatic time-out of user access if left idle, identification and password required to reopen;
- ✓ accounts are monitored and access revoked when several erroneous passwords are entered, log file of events (monitoring of break-in-attempts);
- ✓ issuing and safeguarding of identification codes and secure tokens;
- ✓ strong password requirements (minimum length, use of special characters, re-use etc.);
- ✓ protection against external access by means of state-of-the-art web application firewalls and network access controls.
- ✓ employee access will be safeguarded by a VPN connection with multi-factor login.
- ✓ all access to data content on machines or computer systems is logged, monitored, and tracked.

3. Access Control to Use Specific Areas of Data Processing Systems

The Company commits that the persons entitled to use its data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that customer data cannot be read, copied or modified, or removed without authorization. This will be accomplished by:

- ✓ employee policies and training in respect of each employee's access rights to personal data;
- ✓ access rights are granted exclusive to specific job and/or functions;
- ✓ monitoring capability in respect of individuals who delete, add or modify personal data;
- ✓ effective and measured disciplinary action against individuals who access personal data without authorization;
- ✓ release of data to only authorized persons;
- ✓ control of files, controlled and documented destruction of data; and
- ✓ policies controlling the retention of back-up copies.

4. Transmission Control

The Company implements suitable measures to prevent customer data from being read, copied, altered, or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of customer data by means of data transmission facilities is envisaged. This is accomplished by:

- ✓ use of state-of-the-art firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- ✓ the use of 128bit SSL-encryption for all https-connections;
- ✓ implementation of secure two-factor VPN connections to safeguard the connection to the internet, if applicable;
- ✓ encryption of customer data by state-of-the-art encryption technology; and
- ✓ constant monitoring of infrastructure (i.e., ICMP-Ping at network level, disk space examination at system level, successful delivery of specified pages at application level).

5. Input Control into Data Processing Systems

The Company implements suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or removed. This is accomplished by:

- ✓ an authorization policy for the input of data into hosted service, as well as for the reading, alteration and deletion of stored data;
- ✓ authentication of authorized personnel;
- ✓ protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- ✓ utilization of user codes (passwords and tokens);
- ✓ automatic log-off of user ID's that have not been used for a substantial period of time;
- ✓ logging or otherwise evidencing input authorization; and
- ✓ electronic recording of entries.

6. Instructional Control of Personal Data

The Company ensures that customer data may only be processed in accordance with a Company customer agreement together with any reasonable and relevant instructions received in writing from authorized customer personnel from time to time which may be specific instructions or instructions of a general nature as set out in a Company customer agreement or as otherwise agreed between customer and Company during the term of a Company customer agreement. This is accomplished by binding policies and procedures for Company employees.

7. Availability Control

The Company implements suitable measures to ensure that customer data are protected from accidental destruction or loss. This is accomplished by:

- infrastructure redundancy: reporting data is stored on hardware with redundant disks subsystem backed up in real time with off-site replication backups.

8. Separation of Processing for Different Purposes

The Company implements suitable measures to ensure that data collected for different purposes can be processed separately. This is accomplished by:

- ✓ access to data is separated through multiple diverse applications for the appropriate users.
- ✓ customer data is separated from development and testing environments through various network and logical controls; and
- ✓ interfaces, batch processes, and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

9. Sub-processors

The Company engages various sub-processors in connection with its cloud infrastructure. The Company ensures that it has robust contractual provisions in place to ensure compliance by such sub-processors with the organizational security measures outlined herein.

APPENDIX 2
LIST OF AUTHORISED SUB-PROCESSORS

AMAZON WEB SERVICES ("AWS")

<i>Address</i>	440 Terry Ave N Seattle, WA 98109-5210 United States
<i>Service Description</i>	Broadbean uses AWS cloud infrastructure to host services which store and process client data. All services are hosted in AWS EU region.
<i>Processing location</i>	Ireland
<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU
<i>Additional Standards and Certifications</i>	We have a GDPR compliant data processing agreement in place between Broadbean and AWS. A copy of this contract is available on request. AWS is a leading cloud hosting provider operating to the highest standards of data protection and security. Further information can be found at: https://aws.amazon.com/compliance/eu-data-protection/ https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf Details of relevant AWS certifications can be found at: https://d0.awsstatic.com/whitepapers/compliance/AWS_Certifications_Programs_Reports_Third-Party_Attestations.pdf

GOOGLE

<i>Address</i>	1600 Amphitheatre Pkwy Mountain View, CA 94043 United States
<i>Service Description</i>	Sub-processor for email and document retention
<i>Processing location</i>	Ireland
<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU
<i>Additional Standards and Certifications</i>	

SAP

<i>Address</i>	One Alliance Center 3500 Lenox Rd NE, Suite T12 Atlanta, GA 30326 United States
<i>Service Description</i>	Sub-processor for managing and analyzing customer interactions and data.
<i>Processing location</i>	United States
<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU and transferred to the US pursuant to Standard Contractual Clauses
<i>Additional Standards and Certifications</i>	

SENGRID

<i>Address</i>	1801 California Street Suite 500 Denver, CO 80202 United States
<i>Service Description</i>	Sub-processor for email notifications.
<i>Processing location</i>	United States
<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU and transferred to the US pursuant to Standard Contractual Clauses
<i>Additional Standards and Certifications</i>	

MICROSOFT

<i>Address</i>	1 Microsoft Way Redmond, WA, 98052 United States
<i>Service Description</i>	Sub-processor for data warehousing.
<i>Processing location</i>	United States
<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU and transferred to the US pursuant to Standard Contractual Clauses
<i>Additional Standards and Certifications</i>	

ORACLE

<i>Address</i>	2300 Oracle Way Austin, TX 78741 United States
<i>Service Description</i>	Sub-processor for enterprise resource planning, supporting automation and processes in finance, procurement and fulfillment services.
<i>Processing location</i>	United States
<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU and transferred to the US pursuant to Standard Contractual Clauses
<i>Additional Standards and Certifications</i>	

WORKDAY

<i>Address</i>	6110 Stoneridge Mall Road Pleasanton, CA 94588 United States
<i>Service Description</i>	Sub-processor for human capital and human resources management.
<i>Processing location</i>	United States
<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU and transferred to the US pursuant to Standard Contractual Clauses
<i>Additional Standards and Certifications</i>	

SALESFORCE

<i>Address</i>	Salesforce Tower 415 Mission Street, 3rd Floor San Francisco, CA 94105 United States
<i>Service Description</i>	Customer Relationship Management System
<i>Processing location</i>	United States
<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU and transferred to the US pursuant to Standard Contractual Clauses
<i>Additional Standards and Certifications</i>	

DOCUSIGN

<i>Address</i>	221 Main Street, Suite 1550 San Francisco, CA 94105 United States
<i>Service Description</i>	Contract Lifecycle Management and Electronic Signatures
<i>Processing location</i>	United States
<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU and transferred to the US pursuant to Standard Contractual Clauses
<i>Additional Standards and Certifications</i>	

PENDO.IO INC.

<i>Address</i>	301 Hillsborough St., Suite 1900 Raleigh, NC 27603 United States
<i>Service Description</i>	Pendo provides a SaaS product pendo.io which collects website usage information and allows Broadbean to analyze product adoption. In doing so it will collect basic contact details of client operators logging in to and using the Broadbean system.
<i>Processing location</i>	US and UK
<i>GDPR Adequacy basis / Safeguards</i>	We have a GDPR compliant data processing agreement in place between Broadbean and Pendo, which includes Modules 1 and 2 of the EU standard contractual clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries.

ARTIRIX LIMITED / PLANDEK

<i>Address</i>	30 Great Guildford St. London SE1 0HS United Kingdom
<i>Service Description</i>	Artirix/Plandek are a data processor we use to provide the back-end database technology for our Internal Search product, sometimes referred to as Talent Search. They operate an instance of Amazon Web Services (AWS above) in which individual client databases of candidates built up using TalentSearch (aka External Search) are stored and in that respect the same security arrangements as listed above for AWS will apply.
<i>Processing location</i>	EU/UK

<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU
---	----------------------

MAILJET SAS

<i>Address</i>	13-13 bis, rue de l'Aubrac 75012 Paris France
<i>Service Description</i>	Mailjet are used as a subcontractor to Broadbean to provide outbound email functionality.
<i>Processing location</i>	EU
<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU
<i>Additional Standards and Certifications</i>	Details of the compliance, security and other measures taken to protect data can be found at: https://www.mailjet.com/gdpr/mailjet-gdpr-compliance/ https://www.mailjet.com/blog/news/what-makes-mailjet-a-secure-email-solution/ https://www.slideshare.net/Mailjet/mailjet-security-presentation-2017

TEXTKERNEL

<i>Address</i>	Nieuwendammerkade 26a5 1022 AB Amsterdam The Netherlands
<i>Service Description</i>	Textkernel provide CV/resume parsing services and semantic candidate matching technology within candidate ranking product
<i>Processing location</i>	EU
<i>GDPR Adequacy basis / Safeguards</i>	Processing within EU

APPENDIX 3 (IF APPLICABLE)

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)¹ 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 I.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 I.A. (hereinafter each “data importer”)

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

- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors 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

¹Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

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

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Intentionally Omitted

Docking clause

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

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, 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 II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses,

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union² (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 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

²The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

- (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) **OPTION 2: GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.³ The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

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 II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice

³This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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 I.C, shall act as competent supervisory authority.

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

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

- (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 safeguards⁴;
 - (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

⁴As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

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 said EU Member State.
- (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

EXPLANATORY NOTE:

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

ANNEX I

A. LIST OF PARTES

Data exporter(s):

Name: The Data Exporter is the Customer that agrees to the Company's services in the Agreement.

Activities relevant to the data transferred under these Clauses: Processing of Customer Data for the purposes of conducting analytics and other Services under the Agreement at the direction of Customer.

Signature and date: This agreement is deemed to be signed and executed by Customer as of the date on which the Customer begins using Company's services.

Role (controller/processor): Controller

Data importer(s):

Name: Veritone, Inc.

Address: 5291 California Avenue, Suite 350, Irvine, CA 92617 USA

Contact person's name, position and contact details: Craig Gatarz, Chief Legal Officer; cgatarz@veritone.com.

Activities relevant to the data transferred under these Clauses: Processing of Customer Data for the purposes of conducting analytics and other Services under the Agreement at the direction of Customer.

Signature and date: This agreement is deemed to be signed and executed by Customer as of the date on which the Customer begins using Company's services.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Consumers whose data is collected by Customer

Categories of personal data transferred

- Contact information, professional or work-related information, education background information.

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.

- Depending on the Veritone services used by Customer, this may include race or ethnic origin, trade union memberships, or biometric data (e.g., voiceprint)

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

- Ongoing

Nature of the processing

- Processing Customer Data for the purposes of fulfilling Company's obligations to the Customer under the Agreement, including performing analytics.

Purpose(s) of the data transfer and further processing

- To process the Customer Data on Company's and its subprocessors' systems outside the European Economic Area.

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

- Until the Agreement between Customer and Veritone is terminated.

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

- Subprocessors will only process Personal Data on Company's behalf to provide services to support Company's provision of services to Customer.

C. COMPETENT SUPERVISORY AUTHORITY

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

Ireland

APPENDIX 4

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	The Exporter is the Customer that agrees to the Company's services in the Agreement.	<p>Full legal name: Veritone, Inc.</p> <p>Trading name (if different): [REDACTED]</p> <p>Main address (if a company registered address): 5291 California Avenue, Suite 350, Irvine, CA 92617 USA</p> <p>Official registration number (if any) (company number or similar identifier): [REDACTED]</p>
Key Contact	<p>Full Name (optional): [REDACTED]</p> <p>Job Title: [REDACTED]</p> <p>Contact details including email: [REDACTED]</p>	<p>Full Name (optional): Craig Gatarz</p> <p>Job Title: CLO</p> <p>Contact details including email: cgatarz@veritone.com</p>
Signature (if required for the purposes of Section 2)	This Exhibit C shall be deemed to be executed by the exporter listed here with the Signature and Date specified within the underlying Data Processing Agreement.	This Exhibit C shall be deemed to be executed by the importer listed here with the Signature and Date specified within the underlying Data Processing Agreement.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	<p>8. <input type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date: [REDACTED]</p> <p>Reference (if any): [REDACTED]</p>
-------------------------	--

		Other identifier (if any): <input type="text"/>				
		Or				
		9. <input checked="" type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	x	x	x	General	30 days	No
3						
4						

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: N/A (Parties are only as listed in Table 1 of this Addendum)

Annex 1B: Description of Transfer: See Description of Transfer as provided in Annex 1B of attached Standard Contractual Clauses

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: N/A for Module 4

Annex III: List of Sub processors (Modules 2 and 3 only): N/A

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	<p>Which Parties may end this Addendum as set out in Section 0:</p> <p><input type="checkbox"/> Importer</p> <p><input type="checkbox"/> Exporter</p> <p><input checked="" type="checkbox"/> Neither Party</p>
--	--

Part 2: Mandatory Clauses

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 0.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 0 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

- a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
- b. Sections 0 to 0 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 0, the provisions of Section 0 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 0 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 0) are made:

- a. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
- b. In Clause 2, delete the words:

“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”;
- c. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;
- d. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
- e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
- f. References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
- g. References to Regulation (EU) 2018/1725 are removed;
- h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
- i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
- j. Clause 13(a) and Part C of Annex I are not used;
- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
- l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

- a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 0, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

its direct costs of performing its obligations under the Addendum; and/or

its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 0 of those Mandatory Clauses.
--------------------------	--