Surveil

Software as a Service (SaaS)

End User License Agreement (EULA)

ITEXACT Limited (Supplier)
Last updated 6/Nov/2024

1. EULA Terms and conditions

1.1. Acceptance of terms and conditions:

(a) The Customer accepts the EULA terms and conditions in effect at the time of supply of the SaaS.

(b) The Supplier may update these terms and conditions at any time and the current version of the terms and conditions as published on Surveil.co will apply to the Customer and be incorporated into all Agreements except that where a Fixed Term applies the updated terms and conditions will not apply for the remainder of the current Fixed Term but will apply for the renewal of that Fixed Term (if any) and any ongoing use beyond the end of the current Fixed Term (as applicable). Supplier will provide one month's written notice of any material change to these terms and conditions.

(c) Without limiting clause 1.1(b), the Customer's continued use of the SaaS confirms the Customer's acceptance to be bound by the latest terms and conditions.

(d) Any additional or different terms that the Customer may stipulate or state in any communication with the Supplier will not be binding on the Supplier or included in the Agreement unless expressly agreed in writing by the Supplier.

(e) The 'Agreement' comprises the Customer Information, Selected Options, Relevant Pricing, these terms and conditions (as updated from time to time under clause 1.1(b) above) and the Support Schedule.

(f) These terms and conditions apply to customers that purchase SaaS (or on whose behalf SaaS is purchased) and if there is a trial period available, these terms and conditions also apply to that trial period.

(g) The SaaS is available from the Supplier directly and from Authorized Partners and is available at various Purchase Locations. Regardless of where the purchase is made, these terms and conditions apply as between the Supplier and the Customer.

(h) All capitalized terms used in these terms and conditions have the meanings given to them in the definition section in clause 19.

(i) Where someone other than the Customer purchases SaaS on behalf of the Customer that person is deemed to have authority to accept these terms and conditions for the Customer.

2. Trial

2.1. If a Trial is available to the Customer and the Customer elects to use the SaaS for a Trial, the Customer acknowledges that use of SaaS for the Trial is subject to these terms and conditions.

2.2. Trial period

(a) The Trial will commence when the Trial SaaS is made available to the Customer. In order for the Trial SaaS to be available to the Customer, the Customer will need to follow the steps outlined to the Customer by the Supplier, the Authorized Partner or at the Purchase Location, and accept these terms and conditions. The Customer acknowledges that the Trial is for the version of SaaS made available under the free trial offer, as hosted by the Supplier. The free trial will end on expiration of the Trial Period, unless terminated earlier under these terms and conditions.

2.3. Provisioning for Trial

(a) The Supplier will provide the Trial SaaS to the Customer in accordance with these terms and conditions. The Supplier will:

(i) provide the Customer with access to the Trial SaaS;

(ii) provide assistance with use of the SaaS as reasonably requested by the Customer (or the Supplier will procure the Authorized Partner to provide assistance). The assistance will be available from the Customer during the hours notified by the Supplier, or the hours notified by the Authorized Partner or at the Purchase Location (as applicable). If no hours are notified, the Supplier or relevant Authorized Partner will use reasonable endeavours to provide assistance during their working day.

2.4. Common terms apply: Except for clauses 3, 5 and 6, all clauses of these terms and conditions apply to Trials (in addition to this clause 2).

3. SaaS

3.1. Provision of SaaS: The Supplier will provide the SaaS to the Customer in accordance with the Agreement. The SaaS is provided to the Customer on a non-exclusive basis and the Customer's right to use the SaaS is not transferable. The Supplier will provide log on access to the Customer to enable the Customer to access and use the SaaS.

3.2. SaaS Hosting and Availability: The Supplier provides the SaaS bundled with the Hosting. The Supplier's commitment to SaaS availability is the Monthly Uptime Commitment, which

applies subject to the Exception Factors. Where emergency maintenance is necessary or where unplanned outages occur, this will be notified to the Customer as soon as possible after coming to the Supplier's attention. Where the Supplier does not meet the Monthly Uptime Commitment, and the failure to meet the Monthly Uptime Commitment is not due to any of the Exception Factors:

(a) Service Credit may apply; and

(b) the Customer may submit a Claim to the Supplier.

If the Supplier, following its assessment of the Claim, determines that the Monthly Uptime Commitment was not met in the relevant period (and that this was not due to any Exception Factors), a Service Credit will apply. The total aggregate amount of Service Credits issued by the Supplier in any given calendar month will not exceed 10% of the total monthly fees paid by the Customer for the affected Service in that month. (Service Credits are not available for every SaaS, refer definition of 'Service Credit' in clause 19).

SaaS Availability: The availability of the SaaS is dependent on factors outside of the Supplier's control and as such the Supplier cannot and does not warrant that the SaaS will be continuously available or available without interruption.

3.3. Exception Factors: The Exception Factors are:

(a) Planned Maintenance;

(b) lack of availability or outages of telecommunications networks (Supplier to provide evidence);

(c) a network or device failure external to the Supplier's or its third-party provider's data centers, including at Customer's site or between the Customer's site and the Supplier's or third party's data centers;

(d) issues resulting from the Customer's use of infrastructure (including IaaS), software or services (other than the SaaS) including issues related to dependencies on the Customer's Integrated Services and Products;

(e) any third-party act, omission or circumstance which results in unavailability of the SaaS, whether malicious or not (other than where the third party is a subcontractor engaged by the Supplier); and

(f) a Force Majeure Event.

3.4. Security Breach

(a) Without limiting any other legal obligations that the Supplier may have in the event of a security breach, the Supplier represents that it has used and will continue to

use reasonable endeavours in designing and/or utilizing the SaaS Systems and in operating and managing the SaaS so as to minimize the risk of a Security Breach.

(b) In the event of any Security Breach:

i. the Supplier will, subject to all applicable laws, notify the Customer as soon as practicable after the Supplier becomes aware of the Security Breach;
ii. the Customer will notify the Supplier as soon as practicable, but no later than 24 hours after the Customer becomes aware of the Security Breach;

(c) subject to all applicable laws, immediately following notification of a Security Breach under clause 3.4(a) or (b) above, the parties will coordinate with each other to investigate the Security Breach. The Supplier will cooperate with the Customer in the Customer's handling of the matter, including, without limitation by assisting with any investigation, providing the Customer with physical access to the facilities and operations affected to the extent reasonably practical, facilitating interviews with the Supplier's employees and others involved in the matter and making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise reasonably required by Customer.

3.5. Data

(a) The Customer warrants that the Customer has the right and authority to deal with the Data in the manner contemplated by the Agreement.

(b) The Customer is responsible for:

i. all Data entry requirements; and
ii. except as expressly provided otherwise in the Agreement, for all aspects of the Customer's access and use of the SaaS; and
iii. managing the Permitted Users and ensuring their compliance with the obligations of this Agreement in respect of their use of the SaaS and managing any changes to the Permitted Users;
iv. ensuring that Permitted Users keep all login details for the SaaS confidential and do not share their login details; and
v. ensuring that, in using the SaaS, the Customer and all Permitted Users comply with all applicable laws. To the extent permitted by law, the Supplier accepts no responsibility for ensuring that use of the SaaS will result in the Customer complying with applicable laws or enable the Customer to comply with applicable laws (including for example and without limitation, laws requiring records to be stored in a particular jurisdiction).

(c) Nothing in the Agreement transfers ownership of the Data to the Supplier or to any Authorized Partner.

(d) All Data is available to the Customer:

i. for the term of the Agreement, via the SaaS;
ii. on request to the Supplier at any time during the term of the Agreement and for a period of 1 Month following expiration or termination of the Agreement.

3.6. Support: The Supplier or Authorized Partner will provide assistance in resolving issues in respect of the Customer's access or use of the SaaS, in accordance with the Support Schedule.

3.7. Common terms apply: Except for clause 2, all clauses of these terms and conditions apply to the SaaS (in addition to this clause 3).

3.8. The Customer acknowledges and agrees that Bulk Transfers of Data may be necessary for the provision of the SaaS and related services, and the Supplier will take all necessary steps to ensure that such transfers are secure and comply with the terms of this Agreement. Where an Authorised Partner is acting on behalf of the Customer, the Customer confirms that the Authorised Partner has the authority to include the Customer's data in a bulk transfer.

3.9. The Supplier will ensure that appropriate safeguards are in place for bulk transfers of Data, including the use of Standard Contractual Clauses or other approved mechanisms under the respective Data Protection Laws.

3.10. Data Analytics and Benchmarking

3.10.1. Subject to clause 7 (Data Protection) and clause 9 (Confidential Information) the Customer grants to the Supplier during the term of this Agreement the worldwide, non-exclusive, non-transferable right to collect, copy, analyse (including by AI analytics), use, adapt, exploit and disseminate the Usage Data (provided this is aggregated and de-identified), in the course of its business activities for benchmarking and other services. Supplier will ensure no Personal Data can be isolated or exposed in this process.

3.11. AI Features

3.11.1. From time to time, Supplier may introduce features and capabilities as part of the SaaS that utilise AI Features. Customer may upload Input, and receive Output generated by the AI Features based on the Input. Customer is solely responsible for the Input and for ensuring that it complies with Applicable Laws and these terms and conditions.

3.11.2. Subject to clause 7 (Data Protection) and clause 9 (Confidential Information) and the restrictions in clause 3.13, the Supplier hereby grants Customer a limited, revocable, non-exclusive, non-transferable and non-sublicensable license to use the AI Features during the term of the term of this Agreement. Supplier and its licensors exclusively

own all right, title, and interest in and to the AI Features and the Output, including all associated intellectual property rights. To the extent permitted by applicable third-party terms of service, Supplier hereby grants to Customer a non-exclusive, sublicensable, worldwide license in and to the Output during the term of this Agreement solely in its business activities and subject to the restrictions in clause 3.1 2 and 3.13.

3.12. Restrictions. Customer will not, unless permitted by express written consent from Supplier:

i. Use any Supplier IP or the Output in connection with the development of any software program, such as competing service including, without limitation, training any artificial intelligence tools for any purpose, such as the purpose of developing content or large language model training; or

ii. use Supplier Content or the Output in connection with any third-party Artificial Intelligence tools for the purpose of deriving any profit or other financial gain.

3.13. EU AI Restrictions (EU Customers only). The Customer will not, unless permitted by express written consent from Supplier:

i. use Supplier IP, AI Features, AI Content or Output in any manner that violates applicable laws, regulations or guidelines, including but not limited to the EU AI Act;

ii. sub-license, sell, lease or otherwise distribute AI Features, AI Content or Output to any third parties.

3.14. Transparency, Accountability, Governance & Oversight. The Supplier will ensure that:

i. AI features are deployed in a manner that is transparent, traceable, and auditable;

ii. clear and understandable information about the AI System's capabilities, limitations, and potential risks is available to Customers;

iii. it implements appropriate data governance measures to ensure the accuracy, relevance, and proportionality of the AI Features, and conducts regular risk assessments to identify and mitigate potential risks; and

iv. AI Features are deployed with appropriate human-machine interface tools to enable effective human oversight, including the ability to monitor, interpret, override, or stop the system when necessary.

4. SaaS Dependencies

(a) The Customer acknowledges that the SaaS is or may be dependent on proper implementation and availability and correct functioning of the Customer's Integrated Services and Products.

(b) Neither the Supplier nor any Authorized Partner has any responsibility or liability to the Customer, and in any event no obligation to refund or reduce amounts paid by the Customer, for incorrect or unexpected functioning, or failure, of the SaaS where that incorrect or unexpected functioning, or failure, is directly or indirectly due to incorrect or inappropriate implementation or incorrect functioning, or lack of availability of the Customer's Integrated Services and Products.

5. Charges and payment

5.1. The Customer will pay the Relevant Pricing for the SaaS to the Supplier, the Authorized Partner or via the Purchase Location (as applicable) in accordance with the timing agreed in writing between the Customer and the Supplier, between the Customer and the Authorized Partner or as accepted by the Customer at the Purchase Location. The Supplier reserves the right to suspend access to the SaaS if payment is not received within the agreed timeframe.

5.2. All applicable value added taxes will be charged and payable in addition to the Relevant Pricing.

5.3. Subject to clause 5.4, the Customer will pay all invoices in full, without setoff, counterclaim or deduction of any kind, on or before the due date.

5.4. If the Customer wishes to dispute an invoice, it must notify the Supplier in writing within 14 days of the date of the invoice and provide details of the dispute. The Customer may withhold payment of the disputed part of an invoice only and must pay that part (or any amount subsequently agreed or determined to be the correct amount owing) promptly on resolution of the dispute.

5.5. Without the Supplier waiving any other right or remedy it may have, if any amount due is not paid by the Customer by the due date, the Supplier may:

(a) charge the Customer interest calculated at 10% on the balance of the amount due by the Customer from the due date until payment is received in full by the Supplier; and/or

(b) charge the Customer all collection costs reasonably incurred by the Supplier in collection of the amount outstanding (including solicitor and/or collection agency fees); and/or

(c) suspend supply of the SaaS until the outstanding amount is paid in full. The Supplier will give 10 Working Days' notice in writing of its intention to suspend delivery under this clause.

5.6. The Relevant Pricing may be changed by the Supplier on the Supplier giving at least six weeks' written notice (by email) to the Customer of the new charges that will apply except that where a Fixed Term applies, the new pricing will not apply until expiration of the current Fixed Term.

6. Term

6.1. The Agreement commences (and provision of the SaaS and Support Services commences) when the Customer purchases the SaaS, and the Agreement will continue:

(a) where there is no Fixed Term, until terminated under clause 6.2 or clause 11;

(b) where there is a Fixed Term, for the Fixed Term unless terminated under clause 6.3 or clause 11.

6.2. In addition to the parties' rights of early termination under the Agreement or otherwise at law, where there is no Fixed Term the Agreement may be terminated by the Customer at any time:

(a) on written notice to the Supplier, or where the purchase was made from an Authorized Partner on written notice to that Authorized Partner; or

(b) through the termination processes at the Purchase Location,

with the termination taking effect at the end of the month in which the Supplier or Authorized Partner (as applicable) confirms receipt of the Customer's termination request. The Customer shall pay all fees for the entire month in which the termination notice is provided.

6.3. In addition to the parties' rights of early termination under the Agreement or otherwise at law, where a Fixed Term applies (including where the Customer selects a Fixed Term at the Purchase Location as a Selected Option (where available)), the Agreement will continue until expiration of the Fixed Term. On expiration of the Fixed Term the Agreement will, subject to clause 5.4, automatically continue for further periods each of the duration of the Fixed Term (or such shorter period as may apply following the initial Fixed Term) on the same terms and conditions (unless updated as provided for under clause 1.1(b)) unless at least one month prior to the expiration of the current Fixed Term one party notifies the other party in writing that the Agreement is to terminate on expiry of the current Fixed Term.

7. Data Protection

7.1. Where Data Protection Laws apply, the Data Protection Schedule attached to these terms and conditions applies. Where Data Protection Laws do not apply, the Data Protection Schedule may not be attached or if it is attached in any event does not apply.

8. Intellectual Property

8.1. All Intellectual Property in:

(a) the SaaS; and

(b) the software, processes, methodology and know-how used by the Supplier in its performance of the Agreement;

is the property of the Supplier (or its licensors) and nothing in the Agreement operates to change that ownership.

8.2. The Customer must not, nor may the Customer permit any other person to do any of the following, or attempt to do so:

(a) copy, alter, modify, reverse assemble, reverse compile, reverse engineer, decompile, disassemble, or enhance the SaaS Systems; or

(b) permit or enable users other than Permitted Users to access or use the SaaS; or

(c) provide the SaaS to any users through operation of a bureau or like service; or

(d) resell, rent, lease, transfer, sublicense or otherwise transfer rights to use the SaaS; or

(e) use the SaaS in any way that could damage or interfere with the SaaS Systems in any way;

(f) use the SaaS otherwise than in the manner in which the SaaS is designed to be used;

(g) use the SaaS in any way that could interrupt, damage or otherwise interfere with use of the SaaS by any other customers;

(h) do any act which would or might invalidate or be inconsistent with the Supplier's Intellectual Property rights.

8.3. The Customer must notify the Supplier of any actual, threatened or suspected infringement of any Intellectual Property right and of any claim by any third party that any use of the SaaS infringes any rights of any other person, as soon as that infringement or claim comes to the Customer's notice. The Customer must (at the Supplier's expense) do all such things as may reasonably be required by the Supplier to assist the Supplier in pursuing or defending any proceedings in relation to any such infringement or claim.

8.4. The Customer indemnifies the Supplier its affiliates, and their respective officers, directors, employees, and agents against any loss, costs, expenses, demands or liability whether direct, indirect or otherwise, including reasonable legal fees, and whether arising in contract, tort (including negligence), equity or otherwise, arising out of or in any way connected with the Customer's use of the SaaS or any breach of this Agreement by the Customer or any Permitted User.

9. Confidential Information

9.1. The parties recognise and acknowledge the confidential nature of the Confidential Information.

9.2. Neither party may use or disclose any Confidential Information other than:

(a) to its employees, directors or contractors to the extent necessary in the performance of the Agreement; or

(b) with the express prior written consent of the other party; or

(c) to its professional advisers.

10. Warranties

10.1. Each party warrants to the other that it has authority to enter into and perform and the ability to perform its obligations under the Agreement.

10.2. With the exception of the warranties given under clauses 10.1, all warranties, terms and conditions (including without limitation, warranties and conditions as to fitness for purpose and merchantability), whether express or implied by statute, common law or otherwise are excluded to the extent permitted by law.

10.3. Any warranties made to the Customer under the Agreement extend solely to the Customer.

11. Termination

11.1. The Supplier or the Customer may terminate the Agreement immediately on written notice to the other party if the other party:

(a) breaches any of its obligations under the Agreement and fails to remedy the breach within 20 days of receiving notice requiring the breach to be remedied; or

(b) ceases business or becomes insolvent or goes into liquidation or has a receiver or statutory manager appointed over its assets or ceases to carry on business or makes any arrangement with its creditors.

11.2. On termination of the Agreement:

(a) all amounts due to the Supplier or relevant Authorized Partner will become immediately due and payable;

(b) the Supplier will cease to provide the SaaS to the Customer, and the Customer will cease to have any entitlement to use the SaaS;

(c) the provisions of the Agreement that are by their nature intended to survive termination will remain in full force.

12. Liability

12.1. This limitation does not apply to claims by the Customer for bodily injury or damage to real property or tangible personal property where the Supplier is legally liable for that injury or damage.

12.2. The Supplier's liability under this Agreement is limited to direct loss only, to the amount paid by the Customer in the 12 month period preceding the event giving rise to the claim.

12.3. In no event is the Supplier liable for any indirect loss or for any loss of profits, lost savings, lost revenue, loss of data, business interruption, incidental or special damages, or for any consequential loss.

13. Dispute resolution

13.1. In the event of any dispute arising between the parties in relation to the Agreement, no party may commence any proceedings relating to the dispute (except where the party seeks urgent interlocutory relief) unless that party has complied with the procedures in this clause 13.

13.2. The party initiating the dispute ("the first party") must provide written notice of the dispute to the other party ("the other party") and nominate in that notice the first party's representative for the negotiations. The other party must within fourteen days of receipt of the notice, give written notice to the first party naming its representative for the negotiations ("Other Party's Notice"). Each nominated representative will have authority to settle or resolve the dispute. The parties will co-operate with each other and endeavour to resolve the dispute through discussion and negotiation.

13.3. If the dispute is not resolved within one month following the date of the Other Party's Notice (or such longer period agreed by the parties in writing), either party may utilize any other legal remedies available to it in seeking to resolve the dispute.

14. Consumer guarantees

14.1. The Customer acknowledges that where it is acquiring the SaaS for the purposes of a business, to the extent permitted by the relevant legislation, any statutory consumer guarantees or legislation that are intended to apply to non-business consumers only will not apply.

15. Force majeure

15.1. The Supplier may suspend its obligations to perform under the Agreement if it is unable to perform as a direct result of a Force Majeure Event. Any such suspension of performance must be limited to the period during which the Force Majeure Event continues.

15.2. Where the Supplier's obligations have been suspended under clause 15.1 for a period of 90 days or more, the Customer may immediately terminate the Agreement by giving notice in writing to the Supplier.

16. General

16.1. Entire agreement: The Agreement constitutes the complete and exclusive statement of the agreement between the parties, superseding all proposals or prior agreements, oral or written, and all other communications between the parties relating to the subject matter of the Agreement.

16.2. Waiver: No exercise or failure to exercise or delay in exercising any right or remedy by a party will constitute a waiver by that party of that or any other right or remedy available to it.

16.3. Partial invalidity: If any provision of the Agreement or its application to any party or circumstance is or becomes invalid or unenforceable to any extent, the remainder of the Agreement and its application will not be affected and will remain enforceable to the greatest extent permitted by law.

16.4. Independent contractor: The Supplier is an independent contractor to the Customer and is in all respects independent of the Customer. Nothing in the Agreement constitutes either party a partner, agent, employee or joint venture of the other.

16.5. Suspension: The Supplier may suspend performance of its obligations under the Agreement for so long as it is unable to perform for reasons outside of its control.

16.6. Assignment: The Customer is not permitted to assign its rights under the Agreement.

17. Notices

17.1. Notices from the Supplier to the Customer under the Agreement will be sent to the Customer at the Customer's contact details specified in the Customer Information. The Customer may notify the Supplier of a change to the contact details specified in the Customer Information, on seven days' notice in writing to the Supplier. Notices from the Customer to the Supplier under the Agreement must be sent to the Supplier at the Supplier's relevant office, details included on the Supplier's website.

17.2. Notices sent by email will be deemed received on sending, provided that the sender does not receive an automatic delivery failure notification. Notices sent by post will be deemed received:

(a) on the fifth day following posting if sent and received nationally (not internationally); and

(b) on the fifteenth day following posting if posted internationally.

18. Governing law and jurisdiction

18.1. The Agreement is governed by the laws of England and Wales. The parties hereby submit to the non-exclusive jurisdiction of the courts of England and Wales.

19. Definitions

19.1. In these terms and conditions:

"**AI Content**" means any Input (as defined below) that is processed through or by or because of the AI Features, or Output prompted or generated through or by or because of the AI Features.

"**AI Features**" means the tools used by Supplier which include, use, require or are supported, created or powered by machine learning or Artificial Intelligence, including but not limited to: chatbot, virtual assistant etc.

"**AI System**" means a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence a physical or virtual environment.

"**Artificial Intelligence**" or "AI" means machine-based functionality which has been developed to generate, create or predict Output based on Input.

"Agreement" means this End User Licence Agreement;

"Authorized Partner" means a third party that has been authorized by the Supplier to sell the SaaS;

"Bulk Data Transfer" means the transfer of large volumes of Data, including the Customer's Data and Personal Data, to a third party or across borders, subject to compliance with applicable Data Protection Laws.

"Claim" means a claim, submitted by the Customer to the Supplier in writing, that the Monthly Uptime Commitment has not been met (claims are subject to the Supplier determining whether or not an Exception Factor applied);

"Confidential Information" means any proprietary information, know-how and data disclosed or made available by one party to the other party but does not include any information which:

(a) is in the public domain without any breach of the Agreement;

(b) on receipt by the other party is already known by that party;

(c) is at any time after the date of receipt by the other party, received in good faith by that party from a third party;

(d) required by law to be disclosed by the other party;

"Customer" means the customer named in the Customer Information;

"Customer Information" means the customer name, email address and any other contact information submitted by or on behalf of a customer:

(a) to the Supplier or Authorized Partner in the course of agreeing to purchase (or agreeing to a Trial) of the SaaS;

(b) at a Purchase Location in the course of agreeing to purchase (or agreeing to a Trial) the SaaS;

"Customer's Integrated Services and Products" means services or products (including third party services or products) which are integrated (in any way) by or for the Customer with the SaaS, regardless of who undertakes that integration work or how it is undertaken;

"Data" means the Customer's data that is entered by the Customer and processed in the course of provision of the SaaS and includes where the context permits, the 'Personal Data' (as defined in the attached GDPR and Data Protection Schedule);

"Data Protection Legislation" means all applicable data protection and privacy legislation in force from time to time in the UK and EU including without limitation the UK GDPR, the EU GDPR, the Data Protection Act 2018 (and regulations made thereunder (DPA 2018), and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended, the US Data Protection Legislation; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data.

End User License Agreement or EULA means this whole document and its applicable scope.

"EU AI Act" means the regulation (EU) 2024/1689;

"EU GDPR" means the General Data Protection Regulation (EU) 2016/679;

"Exception Factors" means factors the existence of which mean the Supplier cannot ensure availability of the SaaS, as described in clause 3.3;

"Fixed Term" (if any) means:

(a) the fixed term for supply of the SaaS, agreed in writing between the Supplier or relevant Authorized Partner and the Customer; or

(b) the fixed term selected by the Customer in the Selected Options;

"Force Majeure Event" means any war, riot, third party strike, natural disaster or other circumstance of a similar nature that is outside of the control of the affected party;

"Hosting" means the Standard Hosting or if applicable, the Selected Hosting and is subject to the Monthly Uptime Commitment;

"Input" means any data or other information Customer or Customer's User provides to Supplier to be processed by an AI Feature.

"Intellectual Property" includes all copyright, trademarks, designs, patents, domain names, concepts, know-how, trade secrets, logos and all other similar property and rights whether registered or unregistered;

"Monthly Uptime Commitment" (where applicable) means the monthly uptime commitment made by the Supplier for the SaaS, relevant to the Hosting, as notified in writing by the Supplier or Authorized Partner or by written notification at the Purchase Location, prior to purchase;

"Output" means any data, information, functionality, or action, carried out, prompted, predicted or generated by an AI Feature using the Input.

"Permitted Users" means:

(a) employees, directors or contractors of the Customer; and

(b) where the Selected Options include options for selecting the number of permitted users, not more than the number of employees, directors or contractors selected;

"Planned Maintenance" means maintenance on all or any part of the SaaS Systems and if applicable to the Agreement will be undertaken at times notified to the Customer in writing;

"Purchase Location" means any internet site from which the SaaS is available for purchase;

"Relevant Pricing" means the pricing for the SaaS that is notified in writing to the Customer by the Supplier or by the relevant Authorized Partner prior to the purchase by the Customer or made available at the Purchase Location, and:

(a) includes Standard Hosting or Selected Hosting as applicable;

(b) where Selected Options apply, means or includes (as applicable) the pricing for the Selected Options;

"SaaS" means the software-as-a-service supplied by the Supplier and selected by the Customer by agreement with the Supplier or an Authorized Partner or at the Purchase Location, as modified from time to time by the Supplier;

"SaaS Systems" means, as the context permits, the software used by the Supplier to provide the SaaS and/or the equipment on which that software is installed (whether this is the Supplier's software or equipment or is third party software or equipment);

"Security Breach" means access or disclosure of the Data to or by anyone other than the Permitted Users where the access or disclosure occurs through bypassing the security mechanisms of the SaaS Systems;

"Selected Hosting" if there are hosting options other than Standard Hosting, means the hosting selected by the Customer from the options offered by the Supplier to the Customer;

"Selected Options" means, if there are options to choose from for provision of the SaaS, the options for provision of the SaaS selected by the Customer by agreement with the Supplier, an Authorized Partner or at the Purchase Location (the options may include for example, the Selected Hosting (if applicable), Support Services options, the maximum number of users or the term for which the SaaS is to be provided);

"Service Credit" means the Supplier's service credits (if any), details of which are available on request from the Supplier or relevant Authorized Partner (as applicable) or specified at the Purchase Location;

"Supplier IP" means the Intellectual Property rights pertaining to the Supplier or its licensors incorporated in the SaaS.

"Support Schedule" means the support schedule which is either attached to these End User terms and conditions or separately provided by the Supplier or Authorized Partner or made available at the Purchase Location, prior to purchase;

"Support Services" means the support services provided under the Support Schedule;

"Standard Hosting" means the Supplier's standard hosting offering for the SaaS as notified by the Supplier to the Customer (or if not notified, details are available on request from the Supplier);

"Trial" (where available) means use of the SaaS, free of charge;

"Trial Period" (where applicable) means the trial period notified to the Customer in writing by the Supplier, Authorized Partner or at the Purchase Location, prior to commencement of the Trial;

"Trial SaaS" (if any) means the version of the SaaS made available by the Supplier at its discretion for a Trial.

"UK GDPR" means the EU GDPR as amended and incorporated into English law in the DPA 2018;

"Usage Data" means data derived from the use by the Customer of the SaaS;

"US Data Protection Legislation" means all applicable federal and state data protection law including the California Consumer Privacy Act 2018 and the California Privacy Rights Act 2020.

20. Interpretation

In these terms and conditions:

(a) reference to the plural includes reference to the singular, and vice versa;

(b) headings inserted for convenience of reference only and do not affect the interpretation of the Agreement.

SUPPORT SERVICES SCHEDULE

This Support Schedule forms part of the Agreement that includes the SaaS End User License Agreement (EULA) terms and conditions.

Defined terms in the SaaS EULA terms and conditions have the same meanings when used in this Support Schedule. Additional defined terms used in this Support Schedule have the meanings given to them in clause 6 of this schedule.

1 Scope

1.1 The Supplier will provide Support Services to the Customer and will respond to Requests for Assistance in respect of the SaaS and/or Hosting, in accordance with the terms and conditions of this Support Schedule.

2 Term

2.1 The term of this Support Schedule is the same as the term of the Agreement.

3 Support Services

3.1 The Supplier will provide Support Services to the Customer and will respond to Requests for Assistance in respect of the SaaS and the Hosting during the Support Hours on receipt of a Service Request from the Customer.

3.2 The Customer will make Service Requests using the procedure specified in:

(a) part 2 of appendix 1, for customers on Basic Support;

(b) part 2 of appendix 2 for customers on Premium Support.

3.3 The Support Services do not include services in respect of any issues arising with access or use of the SaaS that in the Supplier's reasonable opinion are due to:

(a) an Exception Factor; or

(b) the Customer's or any third party's services or products including where the SaaS is dependent on or integrated in any way with those services or products (including the Customer's Integrated Products and Services).

The Supplier may, at its sole discretion, agree to provide assistance with resolving issues of the type described in this clause 3.3 and if and when it does so, the Supplier accepts no responsibility for resolving the issue. The Supplier may charge the Customer at its standard rates for undertaking any work of the type described in this clause 3.3 regardless of whether or not the issue is resolved by that work.

3.4 The Supplier will be available to provide Support Services and to respond to Requests for Assistance:

(a) during the applicable hours specified in:

i. part 1 of appendix 1, for customers on Basic Support;
ii. part 1 of appendix 2, for customers on Premium Support.

(b) if part 1 of appendix 1 or 2 (as applicable) does not specify the support hours, the support hours will be as notified by the Supplier or Authorized Partner (as applicable) or notified at the Purchase Location, prior to purchase of the SaaS.

If no hours are specified or notified as described above in this clause, the Supplier will use reasonable endeavours to provide the Support Services and to respond to Requests for Assistance during the Supplier's usual working day.

4 Charges and payment

4.1 The Support Services are included in the amounts payable under the SaaS End User terms and conditions. The Supplier may charge the Customer, at its standard rates, for any Additional Services. The current standard rates are available on request from the Supplier.

4.2 All invoices issued by the Supplier for Additional Services are due for payment by the Customer 14 days following the date of the invoice.

4.3 Subject to clause 4.4, the Customer will pay all invoices for Additional Services in full, without setoff, counterclaim or deduction of any kind, on or before the due date.

4.4 If the Customer wishes to dispute an invoice for Additional Services, it must notify the Supplier in writing within 14 days of the date of the invoice and provide details of the dispute. The Customer may withhold payment of the disputed part of an invoice only and must pay that part (or any amount subsequently agreed or determined to be the correct amount owing) promptly on resolution of the dispute.

4.5 Without the Supplier waiving any other right or remedy it may have, if any amount due is not paid by the Customer by the due date, the Supplier may:

(a) charge the Customer interest calculated at10% on the balance of the amount due by the Customer from the due date until payment is received in full by the Supplier; and/or

(b) charge the Customer all collection costs reasonably incurred by the Supplier in collection of the amount outstanding (including solicitor and/or collection agency fees); and/or

(c) suspend delivery of further Support Services until the outstanding amount is paid in full. The Supplier will give 10 days' notice in writing of its intention to suspend delivery under this clause.

5 Taxes

5.1 In addition to the amounts due under clause 4, the Customer will pay the Supplier amounts equal to any applicable government taxes or duties however designated, based on the Agreement (or the Support Services or Additional Services provided under it), paid or payable by the Supplier in respect of the foregoing, exclusive however of taxes based on the Supplier's income.

6 Definitions

6.1 Unless the context otherwise requires, in this Support Schedule the following expressions have the following meanings:

"Additional Services" means any services in respect of the following:

(a) services provided in response to any Request for Assistance;

(b) services that the Supplier agrees to provide in respect of Excluded Services;

"Basic Support" means the support described in appendix 1;

"Excluded Services" means the services described in clause 3.3;

"Incident" means the SaaS is not performing in accordance with reasonable use of the SaaS or the Customer is experiencing difficulties in accessing the SaaS which arise due to Hosting issues;

"Incident Request" means a request for Support Services to resolve an Incident;

"Premium Support" means the support described in appendix 2;

"Priority Levels" means the priority levels in part 8 of appendix 2;

"Request for Assistance" means a request for assistance made by the Customer that is not in connection with an Incident and is not Excluded Services;

"Service Desk" means the Supplier's point of contact for receiving Service Requests;

"Service Request" means an Incident Request or Request for Assistance;

"Support Hours" means the hours during which the Supplier will be available to provide Support Services to the Customer, as described in clause 3.4;

"Support Services" means the support services to be provided by the Supplier to the Customer as described in this Support Schedule and includes the Basic Support or Premium Support, and excludes Requests for Assistance and Excluded Services.

Surveil

APPENDIX 1

SUPPORT SERVICES – BASIC SUPPORT

Part 1. Support Hours

Basic Support: Support Hours

UK Business Hours

Part 2. Service Request Procedure

Basic Support - Customer to make Service Request by:

Email:	support@surveil.co

Part 3. Service Desk

Service overview	The service desk provides a point of contact for receiving and managing all Service Requests. This is a second level service desk service.
Scope of service	The Supplier will provide the Service Desk, providing the following in respect of Service Requests: (a) recording the Incident Request or Request for Assistance; (b) initial support; (c) tracking; and (d) keeping the Customer updated on the progress.
Requests for Assistance	Given that Requests for Assistance are separately chargeable, the Supplier will notify the Customer in writing when the Customer issues a Service Request that is a Request for Assistance. The Supplier will provide services to the Customer in response to Requests for Assistance only after providing the written notification above and following receipt of the Customer's confirmation or request to proceed (given in writing or confirmed by the Supplier in writing).

Customer's Responsibilities	The Customer will communicate all Service Requests clearly and completely in an appropriate and effective manner and provide any additional information reasonably required by the Supplier.

Part 4. Response to Service Requests

Basic Support – the Supplier will use reasonable endeavours to resolve Incidents and address Requests for Service reported by the Customer.

DATA PROTECTION SCHEDULE

Data Processing Agreement (DPA)

Under the Agreement, the Customer engages or may engage the Supplier to Process Personal Data on behalf of the Customer. To the extent of that Processing of Personal Data and for the purposes of the Agreement, the Customer is a 'Controller' and the Supplier is a 'Processor' for the purposes of the Data Protection Legislation. As such, Article 28 of the UK GDPR (or EU GDPR as applicable) requires that the details in this schedule are included in the contract between the Customer and the Supplier. Where the relevant legislation is the US Data Protection Legislation, the terms 'Controller' and 'Processor' shall have the same meaning as 'Business' and 'Service Provider' in the CPRA respectively for the purposes of this Data Protection Schedule.

The parties must set out the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of data subjects – see appendix 1 to this schedule. If the Supplier determines the purposes and means of Processing, the Supplier is considered a 'Controller' in respect of that Processing in which case the Supplier needs to consider and address the different and additional provisions of the GDPR that apply.

The terms used in this schedule have the meanings given to them in clause 13 of this schedule. Capitalized terms used in this schedule that are not defined in clause 13 of this schedule have the meaning given to them in the Data Protection Legislation or in the Agreement.

Headings used in this schedule are for ease of reference only and are not intended to influence the interpretation of a clause.

1 **Processing of Personal Data**

1.1 The Supplier will:

(a) Instructions from Customer: in providing Services under this Agreement, Process Personal Data only on the Customer's documented instructions (as provided in clause 2 and in appendix 1 to this schedule or otherwise in writing) unless required to do so by Data Protection Laws which apply to the Supplier in which case the Supplier will inform the Customer of that legal requirement before Processing unless the Supplier is prohibited from informing the Customer by that law;

(b) Confidentiality: ensure that the Supplier's personnel who are authorised to Process the Personal Data have obligations of confidentiality to the Supplier (including as required in clause 3 below) in respect of the Personal Data or are under an appropriate statutory obligation of confidentiality;

(c) Security: comply with the security obligations in clause 4 below;

(d) Subprocessors: comply with the provisions relating to Subprocessors in clause 5 below;

(e) Data subjects' rights: provide assistance to the Customer with responding to data subjects' rights in accordance with clause 6 below;

(f) Assist Customer: comply with its obligations to assist the Customer in relation to security of Personal Data and data protection impact assessments and prior consultation in accordance with clause 7 below;

(g) Deleting and returning data: after the provision of Services related to Processing of Personal Data has ended, at the choice of the Customer either delete or return to the Customer all of that Personal Data and delete existing copies unless Member or Union State law requires storage of Personal Data in accordance with clause 8 below; and

(h) Compliance and audits: make available to the Customer all information necessary to demonstrate compliance with Article 28 of the UK GDPR (or EU GDPR as applicable) and allow for and contribute to audits including inspections conducted by the Customer or another auditor mandated from time to time, in accordance with clause 9 below. The Supplier will immediately inform the Customer if, in its opinion, an instruction received from the Customer under this clause 1.1(h), infringes the Data Protection Laws.

(i) Data Transfers: Ensure that all transfers of Personal Data from the UK to the US, and from the US to the EU or UK, comply with the applicable Data Protection Laws and are subject to appropriate safeguards as outlined in the Standard Contractual Clauses or other mechanisms approved under the respective Data Protection Laws.

2) Instructions from Customer

2.1 The Customer instructs the Supplier (and authorises the Supplier to instruct each Subprocessor) to:

(a) Process Personal Data; and

(b) in particular, transfer Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with and in compliance with the Agreement and the Data Protection Laws.

2.2 The Customer warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in clause 2.1 on behalf of the Customer.

3 Confidentiality

3.1 The Supplier will take reasonable steps to ensure the reliability of its employees, agents or contractors who may have access to Personal Data, ensuring in each case that access is

limited to those individuals who need to know or need to access the relevant Personal Data, as necessary for the purposes of the Agreement, and to comply with applicable laws in the context of that individual's duties to the Supplier, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4 Security

4.1 Subject to clause 4.2 below, the Supplier will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including amongst other things as appropriate:

(a) the pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

4.2 In assessing the appropriate level of security for clause 4.1 above, the Supplier will take account in particular of the risks of a Personal Data Breach that are presented by the Processing to be undertaken under the Agreement.

4.3 The Supplier will in relation to Personal Data:

(a) implement and maintain appropriate information security to protect Personal Data against:

(i) a Personal Data Breach;
(ii) all other unauthorized or unlawful forms of Processing; and
(iii) any breach of the Supplier's Information Security Obligations in this schedule. The Supplier will (and will ensure that its Sub-processors) provide full cooperation and assistance to the Customer in ensuring that the individuals´ rights under the Data Protection Laws are timely and appropriately addressed for the fulfilment of the Customer's obligation to respond without undue delay to requests by such individuals as required by Data Protection Laws, including the rights of subject access, rectification, erasure, and portability, and the right to restrict or object to certain Processing;

(b) take reasonable steps to inform its staff, and any other person acting under its supervision, of the responsibilities of any Data Protection Laws due to the incidental access to Personal Data, and ensure the reliability of its staff and any other person acting under its supervision

who may come into contact with, or otherwise have access to and Process, such Personal Data.

5 Subprocessors

5.1 The Customer authorises the Supplier to appoint Subprocessors (and permits each Subprocessor appointed in accordance with this clause 5 to appoint Subprocessors) in accordance with this clause 5 and any restrictions in the Agreement.

5.2 The Customer acknowledges that the Supplier engages third parties as Subprocessors to assist with the provision of services and deliverables to customers and that as at the date of these terms and conditions, the Supplier's Subprocessors are Microsoft Azure (based in the US, Europe or the United Kingdom), Surveil Inc. (based in the USA) and UAB Absolute Systems Lithuania (based in Lithuania), both affiliate companies of ITEXACT Limited.

5.3 The Supplier will give the Customer prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within two weeks of receipt of that notice, the Customer notifies the Supplier in writing of any objections (on reasonable grounds) to the proposed appointment, the Supplier will not appoint (nor disclose any Personal Data to) the proposed Subprocessor unless and until it obtains the prior written consent of the Customer.

5.4 With respect to each Subprocessor, the Supplier will:

(a) enter into an agreement with the Subprocessor which includes the same data protection obligations as set out in this schedule (and Appendix 1) and in particular includes sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. If the Subprocessor fails to fulfil its data protection obligations, the Supplier will remain fully liable to the Customer for the performance of that Subprocessor's obligations;

(b) if the Processing by the Subprocessor will involve a Restricted Transfer, ensure that the EU or UK Standard Contractual Clauses (as applicable and set out in Appendix 2 to this schedule) are at all relevant times incorporated into the agreement between the Supplier and the Subprocessor; and

(c) provide to the Customer for review, copies of the Supplier's agreements with Subprocessors (confidential commercial information that is not relevant to the requirements of this schedule may be blacked out) as the Customer may request from time to time.

5.5 Appendix 1 to this schedule sets out certain information regarding the Supplier's Processing of Personal Data, as required by article 28(3) of the UK GDPR or EU GDPR as applicable. The Customer may make reasonable amendments to Appendix 1 by written notice to the Supplier from time to time as the Customer reasonably considers necessary to meet those requirements.

6 Data Subjects' Rights

6.1 Taking into account the nature of the Processing, the Supplier will, by implementing appropriate technical and organisational measures to the extent described in clause 4, assist the Customer to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 The Supplier will:

(a) promptly notify the Customer if the Supplier or any Subprocessor receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and

(b) ensure that the Supplier or relevant Subprocessor does not respond to that request except on the documented instructions of the Customer or as required by applicable laws to which they are subject, in which case the Supplier will to the extent permitted by applicable laws inform the Customer of that legal requirement before the Supplier or relevant Subprocessor responds to the request.

7 Assist Customer

7.1 Assist Customer with Security of Processing:

(a) The Supplier will assist the Customer in respect of the Customer's obligations to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, by complying with the Supplier's obligations under clause 4 of this schedule.

7.2 Assist Customer with notifications of Personal Data Breach

(a) The Supplier will notify the Customer without undue delay if the Supplier or any Subprocessor becomes aware of a Personal Data Breach, providing the Customer with sufficient information to allow the Customer to meet any obligations to report the Personal Data Breach to the relevant Supervisory Authority under the Data Protection Laws (noting that the Customer is required, where feasible, to notify applicable Personal Data breaches to the relevant Supervisory Authority within 72 hours after having become aware of the breach).

(b) The Supplier will co-operate with the Customer and take such reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.3 Assist Customer with communication of Personal Data breach to Data Subject

(a) Where a Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons:

(i) such that the Customer is required to communicate the Personal Data Breach to the Data Subject (including where, despite the conditions referenced in

clause 7.3(a)(ii) below being met, the Supervisory Authority has required the Customer to communicate the Personal Data Breach to the Data Subject), the Supplier will assist the Customer in doing so by providing all relevant information as may be reasonably required by the Customer;

(ii) but despite that high risk, the Customer is not required to communicate the Personal Data Breach to the Data Subject due to certain conditions being met (such as that the Personal Data is encrypted and so unintelligible to any person not authorised to access it), the Supplier will assist the Customer by providing all relevant information as may be reasonably required by the Customer.

7.4 Assist Customer with Data Protection Impact Assessments

(a) The Supplier will provide reasonable assistance to the Customer with any data protection impact assessments which the Customer reasonably considers to be required of the Customer by Article 35 of the GDPR or equivalent provisions of related Data Protection Laws. The Supplier's obligations under this clause 7.4(a) are solely in relation to Processing of Personal Data by the Supplier and taking into account the nature of the Processing and information available to the Supplier.

7.5 Assist Customer with Prior Consultation with Supervisory Authority

(a) The Supplier will provide reasonable assistance to the Customer with prior consultations with Supervising Authorities or other competent data privacy authorities, which the Customer reasonably considers to be required of the Customer by Article 36 of the GDPR or equivalent provisions of related Data Protection Laws. The Supplier's obligations under this clause 7.5(a) are solely in relation to Processing of Personal Data by the Supplier and taking into account the nature of the Processing and information available to the Supplier.

8 Deletion or return of Personal Data

8.1 Subject to clauses 8.2 and 8.3, the Supplier will, within 1 Month of the date of expiration or termination of Services involving the Processing of Personal Data (the "End of Processing Date"), delete and procure the deletion of all copies of the Personal Data.

8.2 Subject to clause 8.3, the Customer may in its absolute discretion by written notice to the Supplier within 1 Month of the End of Processing Date require the Supplier to:

(a) return a complete copy of all Personal Data to the Customer by secure file transfer in such format as is reasonably notified by the Customer to the Supplier; and

(b) delete and procure the deletion of all other copies of Personal Data Processed by the Supplier. The Supplier will comply with any such written request within 1 Month of the End of Processing Date.

8.3 The Supplier may retain Personal Data to the extent required by applicable laws and only to the extent and for such period as required by applicable laws and always provided that the Supplier will:

(a) ensure the confidentiality of all such Personal Data;

(b) ensure that such Personal Data is only processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

8.4 The Supplier will provide written certification to the Customer that it has fully complied with this clause 8 within 1 Month following the End of Processing Date.

9 Audit rights

9.1 Subject to clauses 9.2 to 9.4, the Supplier will make available to the Customer on request all information necessary to demonstrate compliance with this schedule, and will allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of Personal Data by the Supplier.

9.2 Information and audit rights of the Customer only arise under clause 9.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Laws (including, where applicable, article 28(3)(h) of the UK GDPR (or EU GDPR).

9.3 The Supplier may, on reasonable grounds, object to the proposed auditor in which case the Customer will propose an alternate auditor.

(a) The Customer will give the Supplier reasonable notice of any audit or inspection to be conducted under clause 9.1 and will make (and ensure that its auditor makes) reasonable endeavours to avoid causing any damage, injury or disruption to the Supplier's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. The Supplier need not give access to its premises for the purposes of such an audit or inspection for the purposes of more than one audit or inspection in any calendar year, except for any additional audits or inspections which:

(i) the Customer reasonably considers necessary because of genuine concerns as to the Supplier's compliance with this schedule; or
(ii) the Customer is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where the Customer has identified its concerns or the relevant requirement or request in its notice to the Supplier of the audit or inspection.

10 Restricted Transfers

10.1 Where the Services involve a Restricted Transfer:

(a) with the Customer as "data exporter" and the Supplier as "data importer" the parties agree that the appropriate safeguard mechanism is in place in respect of that Restricted Transfer;

(b) with a Subprocessor with Supplier as data exporter and the Subprocessor as data importer, the Supplier will agree to the applicable safeguard mechanism in respect of that Restricted Transfer. Restricted Transfers to Microsoft Azure are subject to the Standard Contractual Clauses between Supplier and Microsoft Azure.

10.2 In respect of Restricted Transfers one or more of the following safeguard mechanisms shall be in place:

(a) US-UK Data Bridge: the UK Extension to the EU-US Data Privacy Framework under Article 45 of the UK General Data Protection Regulation (GDPR) allows for Restricted Transfers from the UK to the US without the need for further safeguards such as those set out in Articles 46 and 49 of the UK GDPR;

(b) UK International Data Transfer Agreement (IDTA) for the transfer of personal data from the UK, issued by the Information Commissioner under section 119A(1) of the Data Protection Act 2018 (DPA 2018);

(c) EU Standard Contractual Clauses.

10.3 Where applicable the IDTA or EU Standard Contractual Clauses will come into effect under clause 10.1 on the later of:

(a) the data exporter becoming a party to them;

(b) the data importer becoming a party to them; and

(c) commencement of the relevant Restricted Transfer.

10.4 There is no requirement for the Supplier and Customer to agree to the IDTA or EU Standard Contractual Clauses (or to include the Standard Contractual Clauses in the Agreement) where the transfer of Personal Data is to an EU Approved Jurisdiction.

11 Order of precedence

11.1 Nothing in this schedule reduces the Supplier's obligations under the Agreement in relation to the protection of Personal Data or permits the Supplier to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this schedule and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

11.2 Subject to clause 11.1, in the event of inconsistencies between the provisions of this schedule and the Agreement, the provisions of this schedule will prevail.

12 Changes in Data Protection Laws

12.1 The Customer may by giving at least 30 calendar days' written notice to the Supplier:

(a) vary the Standard Contractual Clauses, as they apply to Restricted Transfers which are subject to a particular Data Protection Law, as required as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

(b) propose any other variations to this schedule which the Customer reasonably considers to be necessary to address the requirements of any Data Protection Law.

12.2 If the Customer gives notice under clause 12.1(a):

(a) the Supplier will promptly co-operate (and require affected Subprocessors to promptly co-operate) to ensure that equivalent variations are made to the agreements made under clause 5.3; and

(b) the Customer will not unreasonably withhold or delay agreement to any consequential variations to this schedule proposed by the Supplier to protect the Supplier against additional risks associated with the variations made under this clause 12.2.

12.3 If the Customer gives notice under clause 12.1(b),

(a) the parties will promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in the Customer's notice as soon as is reasonably practicable; and

(b) the Customer will not unreasonably withhold or delay agreement to any consequential variations to this Schedule proposed by the Supplier to protect the Supplier against additional risks associated with the variations made under this clause 12.3.

13 Definitions

In this schedule, where not defined in clause 19 of the terms and conditions the following definitions shall apply:

"EU Approved Jurisdiction" means a country (or territory or specified sector within it) or an international organisation which the Commission has decided, under Article 45(3) of the EU GDPR, ensures an adequate level of data protection;

"Contracted Processor" means the Supplier or a Subprocessor

"Data Protection Laws" has the definition in the terms and conditions;

"Data Subject" means an identified or identifiable natural person, or any updated definition of this term from time to time in the Data Protection Laws;

"EEA" means the European Economic Area;

“EU SCCs” means the Standard Contractual Clauses published by the EU Commission in 2021, as set out in Appendix 2 to this schedule.

“Information Security Obligations” means commercially reasonable and appropriate physical, technical and organisational security measures (determined with regard to risks associated with the Processing of Personal Data as part of the Services), including the measures set out in the Agreement and in particular in Appendix 2 to this schedule (where applicable).

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

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, or any updated definition of ‘Personal Data Breach’ from time to time in the Data Protection Laws;

“Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and ‘Process’ has a corresponding meaning;

"Restricted Transfer" means transferring Personal Data outside of the EEA , being: a transfer of Personal Data from the Customer to the Supplier or to a Subprocessor; or an onward transfer of Personal Data from a Contracted Processor to a Contracted Processor, in each case, where such transfer means would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws), in the absence of the applicable Standard Contractual Clauses;

"Services" means the services and other activities to be supplied to or carried out by or on behalf of the Supplier for the Customer under the Agreement;

"Subprocessor" means any person (including any third party, but excluding an employee of the Supplier or any of its sub-contractors) appointed by or on behalf of the Supplier to Process Personal Data on behalf of the Customer in connection with the Agreement;

“Standard Contractual Clauses” means the EU SCCs;

The terms "Member State", "Supervisory Authority" have the meaning given to those terms in the EU GDPR, and corresponding terms have corresponding meanings.

The word "includes" means ‘includes without limitation’, and “including” has a corresponding meaning.

APPENDIX 1 TO DATA PROTECTION SCHEDULE

DETAILS OF PROCESSING OF PERSONAL DATA

This Appendix 1 includes certain details of the Processing of Personal Data as required by Article 28(3) of the UK GDPR (or EU GDPR as applicable) by the Supplier under the DPA.

Subject matter and duration of the Processing of Personal Data

In providing Surveil and other services, it is necessary for the Supplier to hold the personal data of anyone who is a recipient of the services, an employee or officer of a customer and any technician working with the Supplier.

The processing will only be for the duration of the contract or until the personal data is removed from Surveil for any other reason such as the person ending their employment with the Supplier or a customer. The Supplier may retain some personal data for longer if required by law for accounting purposes.

The nature and purpose of the Processing of Personal Data

Personal data is used by Supplier to communicate with customers and to provide the services. Set out below in table format, is a description of all the ways the Supplier will use personal data, and which of the legal bases it relies on to do so.

Purpose/Activity	**Type of data**
To register a new customer	(a) Identity (b) Contact
To process and deliver an order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing & Communications
To manage relationships with a customer which will include: (a) Notifying customers about changes to terms or privacy policy (b) Asking a customer to leave a review or take a survey	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications
To administer and protect the business and the Services (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical

To deliver relevant content and advertisements to customers and measure or understand the effectiveness of the advertising	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical
To use chatbot or AI features on the website or product to provide services and information to customers.	(a) Identity (b) Contact (c) Usage (d) Technical
To use data analytics to improve the website, products/services, marketing, customer relationships and experiences	(a) Technical (b) Usage
To make suggestions and recommendations about goods or services	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile
To process employment applications.	(a) Identity (b) Contact
To provide software to customers, including the Surveil suite of software and SaaS ; and professional and support services, including implementation and configuration.	(a) Identity (b) Contact (c) Technical (d) Usage (f) Technical
To fix problems with products, including answering support questions and resolving disputes.	(a) Identity (b) Contact (c) Profile (d) Usage (f) Technical

The types and categories of Personal Data to be Processed

Supplier may collect, use, store and transfer different kinds of personal data as follows:

- **Identity Data** may include first name, last name, location, employing company, department, given names, job title, office location, username or similar identifier, title.

- **Business Contact Data** includes billing address, state, county, delivery address, email address and telephone numbers.
- **Financial Data** includes bank account and payment details.
- **Transaction Data** includes details about payments and other details of products and services purchased from us.
- **Technical Data** includes internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access this website or as may be configured within the Services.
- **Profile Data** includes username, purchases or orders, preferences, feedback and survey responses.
- **Usage Data** includes information about how individuals use the Services.
- **Marketing and Communications Data** includes preferences in receiving marketing from us and our third parties and your communication preferences.

Supplier also collects, uses and shares **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from personal data but is not considered personal data in law as this data does not directly or indirectly reveal personal identity. For example, Supplier may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature.

Supplier does not collect any **Special Categories of Personal Data** (this includes details about race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about health and genetic and biometric data). Nor do we collect any information about criminal convictions and offenses without specific consent and under a separate agreement.

APPENDIX 2 TO DATA PROTECTION SCHEDULE

EU STANDARD CONTRACTUAL CLAUSES (PROCESSORS) (EU SCCS)

On June 4, 2021, the European Commission released new standard contractual clauses for international data transfers. The following EU SCCs will govern Restricted Transfers of EU personal data made under Article 46(2)(c) of the EU GDPR.

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

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 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 data importer, with the following exceptions:

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

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

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

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

v. Clause 13; Clause 15.1(c), (d) and (e);

vi. Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Not included.

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 Union (2) (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.

(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 1: Not used

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 [*two weeks*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

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 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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(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.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

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

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

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The

data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of 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.

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

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

ANNEX I AND II TO THE EU STANDARD CONTRACTUAL CLAUSES

This Annex forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is:
The Customer
For address details refer to clause 19 of the End User terms and conditions

Data importer
The data importer is:
The Supplier
For address details refer to clause 17 of the End User terms and conditions

Data subjects
The personal data transferred concern the following categories of data subjects:
Data Subject is defined as any user that is part of EntraID (formerly Azure Active Directory).

Categories of data
The personal data transferred concern the following categories of data:
Restricted to minimal size according to GDPR fields in Azure AD.

Property	Description	Processing activities
aboutMe	A freeform text entry field for the user to describe themselves	Data is accessible through API, but not stored
ageGroup	The age group of the user	Data is accessible through API, but not stored
birthday	The birthday of the user	Data is accessible through API, but not stored
businessPhones	The telephone numbers for the user	Data is accessible through API, but not stored
city	The city in which the user is located	This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions
companyName	The company name which the user is associated	This is used to build consolidated reports through our Rules and Tag engine
country	The country/region in which the user is located	This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions
department	The name for the department in which the user works	This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions
displayName	The name displayed in the address book for the user	This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions
employeeId	The employee identifier assigned to the user by the organisation	Data is accessible through API, but not stored
faxNumber	The fax number of the user	Data is accessible through API, but not stored
givenName	The given name (first name) of the user	This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions
imAddresses	The instant message voice over IP (VOIP) session initiation protocol (SIP) addresses for the user	Data is accessible through API, but not stored

interests	A list for the user to describe their interests	Data is accessible through API, but not stored
jobTitle	The user's job title	This is used to build consolidated reports through our Rules and Tag engine
legalAgeGroupClassification	Used by enterprise applications to determine the legal age group of the user	Data is accessible through API, but not stored
mail	The SMTP address for the user	This is a unique identifier for the tool to build its core features around. This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions.
mailNickname	The mail alias for the user	Data is accessible through API, but not stored
mobilePhone	The primary cellular telephone number for the user	Data is accessible through API, but not stored
officeLocation	The office location in the user's place of business	This is a unique identifier for the tool to build its core features around. This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions.
onPremisesDistinguishedName	Contains the on-premises Active Directory distinguished name or DN	This is a unique identifier for the tool to build its core features around. This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions.
postalCode	The postal code for the user's postal address	Data is accessible through API, but not stored
preferredDataLocation	The preferred data location for the user	Data is accessible through API, but not stored
preferredLanguage	The preferred language for the user	Data is accessible through API, but not stored
preferredName	The preferred name for the user	Data is accessible through API, but not stored
schools	A list for the user to enumerate the schools they have attended	Data is accessible through API, but not stored
skills	A list for the user to enumerate their skills	Data is accessible through API, but not stored
state	The state or province in the user's address	This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions
streetAddress	The street address of the user's place of business	This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions
surname	The user's surname	This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions
usageLocation	A two-letter country code	This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions
userPrincipalName	The user principal name (UPN) of the user	This is a unique identifier for the tool to build its core features around. This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions.
ipAddress	IP address of Identity Risk Event or Security Alert	This is a unique identifier for the tool to build its core features around. This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions.
billingProfileName	Name of user defined in the billing profile	This is a unique identifier for the tool to build its core features around. This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions.
customerName	Primary customer contact for the tenant	This is a unique identifier for the tool to build its core features around. This is used to build

		consolidated reports and to help identify a user to the company for IT and Helpdesk functions.
PurchasedBy	Username of purchases for transaction	This is a unique identifier for the tool to build its core features around. This is used to build consolidated reports and to help identify a user to the company for IT and Helpdesk functions.

Purpose of processing
Provision of the services

Subprocessors of personal data

- Microsoft Azure
- UAB Absolute Systems Lithuania
- Surveil Inc.

Technical and operational measures to ensure the security of personal data

(a) the pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.