September 2024

Ativion Services Agreement

www.Ativion.com

ATIVION SERVICES AGREEMENT

This Ativion Services Agreement ("ASA") is between Ativion (as defined in Section 1), and the customer ordering the Ativion Services/identified in the Order ("Customer" or "you").

YOUR CONTINUED USE OF THE SERVICES IS SUBJECT TO THE TERMS OF THIS ASA. BY SIGNING THE ORDER OR ACCESSING AND/OR CONTINUING TO USE THE SERVICES YOU AGREE TO BE BOUND BY IT TO THE EXCLUSION OF ALL OTHER TERMS.

1. DEFINED TERMS.

The following words, when capitalized, have the meaning stated:

"Affiliate" means any legal entity that a party owns, that owns a party, or that is under its common ownership. "Ownership" means, for the purposes of this definition, control of more than a fifty percent interest in an entity.

"Agreement" means, collectively, this ASA and any applicable Order or other addenda which govern the provision of Services.

"Ativion" or **"we"** means the Ativion or Netop Affiliate identified in the Order, or, if none is identified: (i) Impero Solutions, Inc. dba Ativion if your billing address is located in the United States or (ii) Impero Solutions Limited trading as Ativion if your billing address is located outside of the United States.

"Ativion Companies" means: all the entities identified as Ativion Companies listed within the organisation structure available at **www.ativion.com/legal/group-structure/**

"Ativion Group" means Impala Bidco Limited t/a Ativion, a company incorporated in England and Wales with registration number 10878303, registered at Seventh Floor, East West, Tollhouse Hill, Nottingham, NG1 5FS, United Kingdom and its Affiliates consisting of Ativion Companies and Netop Companies.

"Ativion Platform" means an information technology system provided and hosted by Ativion as part of the Services, including any hosted platform or software as a service delivery of the Services.

"Business Day" means Monday through Friday, excluding public holidays in the United States or United Kingdom.

"Confidential Information" means non-public information disclosed by one party to the other in any form that: (i) is designated as "Confidential"; (ii) a reasonable person knows or reasonably should understand to be confidential; or (iii) includes either party's products, customers, marketing and

promotions, know-how, or the negotiated terms of the Agreement; and which is not independently developed by the other party without reference to the other's Confidential Information or otherwise known to the other party on a non-confidential basis prior to disclosure.

"Customer Data" means all data, including Personal Data, which Customer has directly entered or stored into the Ativion Platform on its own or via its employees, students, or users.

"Data Protection Legislation" means all laws and regulations applicable to the Processing of Personal Data under the ASA, including laws and regulations of (a) the European Union, the European Economic Area and their member states, including, without limitation, where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction including, without limitation, (i) the General Data Protection Regulation ((EU) 2016/679) ("GDPR"), (ii) the EU e-Privacy Directive (Directive 2002/58/EC), (iii) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001, and (iv) any national implementing laws, Switzerland, including, without limitation, Swiss Federal Act on Data Protection and implementing regulations, (b) the United Kingdom, including, without limitation, (i) the GDPR as applicable as part of UK domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and as amended by Data Protection, (ii) Privacy and Electronic Communications (EU Exit) Regulations 2019 (the "UK GDPR"), (iii) the UK Data Protection Act of 2018, and the U.S. State Privacy Laws, in each case, as superseded amended or replaced.

"Deliverables" means the tangible or intangible materials which are prepared for your use in the course of performing the Services (specifically excluding Device Agents).

"Device Agents" means any end-user or per-device software or agents provided by Ativion to be used in conjunction with the Services.

"Intellectual Property" means patents, copyrights, trademarks, trade secrets, domain names, database rights, and any other proprietary intellectual property rights, in each case whether registered or unregistered and including all applications (or rights to apply) for, and renewal or extensions of, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

"Netop Companies" mean all the entities identified as Netop Companies listed within the organisation structure available at **www.ativion.com/legal/group-structure/**

"Order" means the document which describes the Services provided pursuant to this Agreement, including any online order, process, or tool through which you request or provision Services or any other notice of written acceptance of an offer to purchase the Services under the conditions of this ASA.

"Personal Data" means all data that is related to an identified or identifiable individual.

"Representatives" means a party's respective service providers, officers, directors, employees, contractors, Affiliates, suppliers, and agents.

"Services" means the Ativion services (including any software) identified in a given Order or otherwise provided subject to the terms of this Agreement, including access to the Ativion Platform.

"User Device" means any individual computer or mobile device of any type which is used by Customer or its students, employees, or users in connection with the Services or on which any Device Agent is installed.

"Use Limits" means any limitations, including any maximum permitted use metrics relating to the maximum number of Device Agents, maximum number of User Devices and maximum number of users of the Ativion Platform, placed on the use of the Services by Ativion as set out in the Order.

"U.S. Privacy Laws" means all applicable data privacy or data protection laws of the United States and each States governing Personal Data, including, but not limited to, California Consumer Privacy Act of 2018, as amended by the California Privacy Right Act of 2020 ("CCPA"), Texas Data Privacy and Security Act (2023 H.B. 4, 88 Reg. Sess (Tex. 2023)), Indiana Consumer Data Protection Act of 2023 (Ind. Code § 24-14 (20023)), the Colorado Privacy Act (Colo. Rev. Stat. §§ 6-1-1301 et seq. and Colo Code Regs. Tit 4 §§904-3 et seq.), the Connecticut Data Privacy Act (Conn. Gen. Stat §§ 42-515 et seq.), Delaware Personal Data Privacy Act (DE HB154), Florida Digital Bill of Rights (Fla. Stat. §§501.701 et seq.), Indiana Consumer Data Protection Act of 2023 (Ind. Code § 24-14 (20023)), Iowa Consumer Data Protection Act (Iowa Code §§ 715D.1 et seq.), Kentucky Consumer Data Protection Act (24RS HB 15), Maryland Online Data Privacy Act (MD SB 541), Massachusetts' Standards for the Protection of Personal Information of Residents of the Common-wealth (201 CM 17: M.G.L. c. 93H), Minnesota Consumer Data Privacy Act (MN HF 4757), Montana Consumer Data Privacy Act (Mont. Code. Ann. §30-14 (2023)), Nebraska Data Privacy Act (L.B. 1074), New Hampshire Privacy Act (NH S.B. 255-FN), New Jersey Data Privacy Act (NJ S.B. 332) , Oregon Consumer Privacy Act (OR 2023 S.B. 619), Tennessee Information Protection Act (Tenn. Code Ann. §§ 47-18-3210 et seq.), Texas Data Privacy and Security Act (2023 H.B. 4, 88 Reg. Sess (Tex. 2023)), the Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101 et seq.), the Virginia Consumer Data Protection Act (Va. Code Ann. §§ 59.1-571 et seq.), Washington My Health My Data Act (RCW §§ 19.373.005 et seq.), Health Insurance Portability and Accountability Act and Accountability Act of 1996 and the regulations promulgated thereunder, including the HITECH Act and Omnibus Rule, as each may be amended from time to time (collectively, "HIPAA"), Children's Online Privacy Protection Act (15. U.S.C. §§ 6501 et seq.)("COPPA"), Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 C.F.R. Part 99)and laws and regulations in the United States, state or federal, of a similar subject matter, as amended or superseded from time to time, as of their respective effective date.

2. SERVICES

2.1. General. Ativion will provide the Services in accordance with the Agreement and all laws applicable to Ativion. Customer must utilize the Services in accordance with any documentation provided by Ativion. Ativion will provide support only to those individuals designated in your account and is not required to provide any support directly to your users.

2.2. Use Limits. Customer may use the Services for educational, wellbeing, and other explicitly permitted purposes only, in accordance with all laws applicable to Customer, and may not resell the Services unless explicitly agreed to by Ativion in writing.

2.3. Device Agents. During the term of the Agreement, Customer may use any software provided by Ativion as part of the Services and may install Device Agents on its users' systems as necessary to receive the benefit of the Services. Device Agents may be subject to additional terms, including third-party terms applicable to use of app stores for mobile devices and any network service provider terms. Customer is responsible for all use of Device Agents in connection with the Services. Fees for Device Agents will be specified on the Order where applicable.

2.4 Representation and Warranties. Ativion represents and warrants to Customer that Ativion will perform the Services using personnel of required skill, experience, and qualifications and in a professional and workmanlike manner in accordance with generally recognized industry standards for similar services and will devote adequate resources to meet its obligations under this Agreement. Ativion further represents and warrants it has the full right, power, and authority to enter into and perform its obligations to this Agreement, and the execution of the Agreement by the individual whose signature is set forth in the Order has been duly authorised by all necessary corporate or organization action.

3. CUSTOMER OBLIGATIONS

3.1. General. You must cooperate with Ativion's reasonable investigation of outages, security problems, and any suspected breach of the Agreement. You are responsible for keeping your account information and permissions current and secure. You agree that your use of the Services will comply with the Use Policy attached as Exhibit A (the "AUP"). You agree that you are solely responsible for the suitability of the Services and you and your users' compliance with any applicable laws, including export control laws, intellectual property laws, and Data Protection Legislation.

3.2. Data Backup. It is the Customer's responsibility to ensure the integrity, security, and confidentiality of Customer Data and to regularly backup and validate the integrity of backups of Customer Data. Ativion has no obligations whatsoever with regards to any data stored on an User Device.

3.3. Representations and Warranties. Customer represents and warrants to Ativion that it owns or otherwise has and will have the necessary rights and consents relating to any data, Intellectual Property, or other inputs it provides to Ativion so that, as received by Ativion, they do not and will not infringe, misappropriate, or otherwise violate any Intellectual Property rights or privacy or other rights of any third party or violate any applicable laws. Customer further represents and warrants it has the full right, power, and authority to enter into and perform its obligations to this Agreement, and the

execution of the Agreement by the individual whose signature is set forth in the Order has been duly authorised by all necessary corporate or organization action.

3.4. Restrictions. Customer shall not:

- (i) modify, copy, duplicate, reproduce, reverse engineer, license or sublicense, transfer or convey the Services or any portion thereof except as otherwise provided for in this Agreement or otherwise without the prior written consent of Ativion;
- (ii) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, or otherwise make available any Services to any third party, including on or in connection with the internet or any time-sharing, service bureau, software as a service, cloud, or other technology or service;
- (iii) use or access the Services for the purpose of building a competitive software or service or for any other competitive purposes;
- (iv) misuse our Services by interfering with their normal operation or attempting to access them using a method other than through the interfaces and instructions provided by Ativion;
- (v) bypass or breach any security device or protection used by the Services or access or use the Services or other than by an Authorised user through the use of his or her own then valid access credentials;
- (vi) circumvent or attempt to circumvent any limitations that Ativion imposes on user accounts (such as using someone else's username and password to get access to Service functionalities not meant for the user in question);
- (vii) probe the vulnerability of any Ativion system or network;
- (viii) use any manual or automated system or software to extract or scrape data from the websites or other interfaces through which Ativion makes the Services available;
- (ix) input, upload, transmit, or otherwise provide to or through the Services, any information or materials that are unlawful or injurious, or contain, transmit, or activate any virus, worm, malware, or other malicious computer code;
- (x) damage, destroy, disrupt, disable, impair, interfere with, or otherwise impede or harm in any manner the Services or Ativion's provision of services to any third party, in whole or in part; or
- (xi) otherwise access or use the Services beyond the scope of the authorisation granted under this Section or in violation of the End User License Agreement found at https://www.ativion.com/legal/EULA/, incorporated herein by reference

4. SECURITY

4.1. Ativion undertakes no responsibility for the security of any User Device. Customer must use reasonable security precautions in connection with its use of the Services. Customer Data is, and at all times shall remain, your exclusive property. Ativion will not use or disclose Customer Data except as materially required to perform the Services or as required by law.

4.2. Customer shall determine which employees, students, and users shall receive access to the Services (the **"Authorised"** users). Ativion shall provide usernames and passwords as necessary for Authorised users at Customer's sole discretion. Ativion shall have no liability whatsoever for unauthorised use of login information of an Authorised

user, unless the unauthorised use was wholly caused by Ativion, its agents, or employees.

For the purposes of this clause, "**Unauthorised**" use shall mean any access or use of the Services by an individual who is not an Authorised user, or any use of the Services that is not in accordance with the terms and conditions of the End User License Agreement, the AUP, and the restrictions set forth in Section 3.4 of this Agreement agreed upon by the Customer and Ativion.

5. INTELLECTUAL PROPERTY

5.1. Pre-Existing. Each party shall retain exclusive ownership of Intellectual Property created, authored, or invented by it prior to the commencement of the Services. If you provide Ativion with your pre-existing Intellectual Property ("Customer IP"), then you hereby grant to Ativion, during the term of the applicable Order, a limited, worldwide, nontransferable, royalty-free, right and license (with right of sub-license where required to perform the Services) to use the Customer IP solely for the purpose of providing the Services. You represent and warrant that you have all rights in the Customer IP necessary to grant this license, and that Ativion's use of such Customer IP shall not infringe on or otherwise misappropriate the Intellectual Property rights of any third party.

5.2. Created by Ativion. Excluding any Customer IP, Ativion shall own all Intellectual Property created as part of providing the Services or contained in the Deliverables. Unless otherwise specifically stated in the Agreement, and subject to your payment in full for the applicable Services, Ativion grants to you, during the term of the applicable Order, a limited, non-exclusive, non-transferable, right and license (without the right to sublicense) to use any Deliverables, and any Intellectual Property (including Device Agents, but excluding any Third-Party Software), provided to you by Ativion as part of the Services for your internal use as necessary for you to enjoy the benefit of the Services. You agree that any usage data, usage metrics, and other general information about your use or operation of the Services may be used and disclosed by Ativion for product improvement and market analysis purposes.

5.3. Third-Party Software. Ativion may provide third party software for your use as part of the Services or to assist in our delivery of the Services ("Third-Party Software"). Unless otherwise permitted by the terms of the applicable license you may not: (i) assign, grant or transfer any interest in the Third-Party Software to another individual or entity; (ii) reverse engineer, decompile, copy or modify the Third-Party Software; (iii) modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Third-Party Software;
or (iv) exercise any of the reserved Intellectual Property rights provided under the laws governing this Agreement. Your use of any Third-Party Software may be subject to additional restrictions identified in the Order or an end-user license agreement or similar terms. Ativion makes no representation or warranty regarding Third-Party Software except that Ativion has the right to use or provide the Third-Party Software and that we are in material compliance with the applicable license

5.4. Infringement. If the delivery of the Services or any portion thereof become the subject of any claim of infringement, then

Ativion, at its sole option, may (i) procure for you the right to continue using the Services as contemplated in the applicable Order; (ii) replace the Services or applicable portion thereof with a substantially equivalent non-infringing service as determined by Ativion; or (iii) modify the Services to make them non-infringing, without materially reducing the features or functionality thereof. If Ativion determines that it is not able to produce the preceding remedies via reasonably or commercially practicable efforts, Ativion may terminate the Order on written notice and will not have any liability on account of such termination except to refund prepaid amounts paid for unused Services (prorated as to portions of Deliverables deemed infringing).

6. FEES.

6.1. Fees. Undisputed fees are due within 30 days of the invoice date. If you have arranged for payment by credit card or bank transfer, we may charge your account on or after the invoice date. If any undisputed payment is 15 or more days late, then we may suspend the Services on written notice. Invoices which are not disputed within 30 days of the invoice date are conclusively deemed accurate. Fees must be paid in the currency identified in the Order.

6.2. Fee Increases. On 30 days' advance written notice, unless otherwise agreed by the parties, Ativion may increase the fees due under any given Order by the greater of (i) 7% or (ii) the percentage change between the United Kingdom's Retail Price Index in the initial month of the applicable Order and the then current month, provided that Ativion may not exercise these rights more than once in any 12-month period. Unless otherwise expressly provided in the applicable Order, fees will automatically increase for each renewal term. If at any time a third-party license or infrastructure provider directly or indirectly increases the fee they charge Ativion for software or services required to deliver the Services, Ativion may increase your fees by the same percentage amount on 90 days' advance written notice.

6.3. Taxes. All amounts due to Ativion under the Agreement are exclusive of any value added, goods and services, sales, use, property, excise and like taxes, import duties, and/or applicable levies (collectively "Tax"). You must pay any Taxes due on Ativion's provision of the Services or provide Ativion with valid evidence of your exemption from such Taxes in advance of invoicing. All fees are due in full without any deduction for any withholding or other taxes except withholding taxes imposed on income attributable to Ativion which you are legally required to withhold and remit to the applicable governmental authority ("Local Withholding Taxes"). You agree to provide Ativion with timely accurate information regarding such Local Withholding Taxes on request.

6.4. Expenses. Except as otherwise included in a given Order, if any of the Services are performed at your site or premises then you agree to reimburse Ativion for the actual substantiated out-of-pocket expenses of our Representatives.

6.5. Free of Charge Services. Where Services are provided free of charge, the provisions of this Agreement continue to apply in full.

7. DISCLAIMERS

7.1. We make no commitment to provide any Services other than the Services stated in the Order. Ativion is not responsible to you or any third party for Unauthorised access to

your Customer Data or for Unauthorised use of the Services that is not solely caused by Ativion's failure to comply with its security obligations in the Agreement.

7.2. At Customer's request, Ativion may provide Services that are not required by the Agreement.Any such Services shall be provided AS-IS, and Ativion disclaims any and all other warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose.

7.3 Ativion may provide free of charge Services. Any such Services shall be provided AS-IS, and Ativion disclaims any and all other warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose.

7.4. TO THE EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS OTHERWISE SPECIFICALLY SET FORTH IN THIS ASA OR THE ORDER, THE SERVICES ARE RENDERED "AS IS", AND ATIVION
AND ITS REPRESENTATIVES DISCLAIM ANY AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

7.5. Ativion makes no representation or warranty whatsoever regarding open source software or with regard to any third-party products or Services which we may recommend for your consideration.

8. TERM AND TERMINATION

8.1. Term. This Agreement shall continue until terminated in accordance with its terms or the termination of the final Order, whichever is later. Unless otherwise stated in the applicable Order, Orders shall automatically renew following their initial term (identified on the Order) for consecutive one-year terms, unless and until either party provides the other with written notice of non-renewal at least 90 days prior to the expiration of the then current term.

8.2. Termination. Either party may terminate the Agreement or the affected Order(s) for cause on written notice if the other party materially breaches the Agreement and does not remedy the breach within 30 days of the other party's written notice describing the breach. If, following the suspension of your Services for non-payment as provided in Section 6.1 (Fees), your account remains overdue for a further 15 days, we may terminate the Agreement or the applicable Orders for breach on written notice. Where Ativion terminates this Agreement for cause as provided for in this Section, all fees due for the then current term shall immediately become due and payable. Upon termination of the Agreement, you will remove any Ativion provided software and Device Agents and any Third-Party Software which has been installed on your (or your users') devices.

8.3. Transition. If you request contemporaneously with any notice of termination (by either party), Ativion shall make the Customer Data available to you for a period of at least 30 days, in a publicly accessible format as it chooses. You agree that you shall promptly retrieve any Customer Data within this time period as required for you to comply with any applicable laws. If Customer Data is not retrieved within 180 days, Personal Data and Customer Data may be destroyed by Ativion.

8.4. Mutual Consent. The exercise by either party of its rights to cancel this ASA pursuant

to its rights under this Section 8 shall be deemed to be exercised with mutual consent. Accordingly, a court order shall not be required.

9. CONFIDENTIAL INFORMATION.

Each party agrees not to use the other's Confidential Information except in connection with the performance or use of the Services, the exercise of its legal rights under this Agreement, or as required by law, and will use reasonable care to protect Confidential Information from Unauthorised disclosure. Each party agrees not to disclose the other's Confidential Information to any third party except: (i) to its Representatives, provided that such Representatives agree to confidentiality measures that are at least as stringent as those stated in this Agreement; (ii) as required by law; or (iii) in response to a subpoena or court order or other compulsory legal process, provided that the party subject to such process shall give the other written notice of at least seven days prior to disclosing Confidential Information unless the law forbids such notice.

10. LIMITATIONS ON DAMAGES

10.1. Direct Damages. Notwithstanding anything in the Agreement to the contrary, except for liability arising from: (i) death or personal injury caused by negligence; (ii) willful misconduct, fraudulent misrepresentation; (iii) willful default; (iv) unlawful acts; or (v) any other loss or damages for which such limitation is expressly prohibited by applicable law, the maximum aggregate monetary liability of Ativion and any of its Representatives in connection with the Services or the Agreement under any theory of law shall not exceed the total amount of fees paid for the Services in the twelve month period immediately preceding the event(s) giving rise to the Claim.

10.2. Indirect Damages. Neither party (nor any of our Representatives) is liable to the other for any indirect, special, incidental, exemplary or consequential loss or damages of any kind. Neither of us is liable for any loss that could have been avoided by the damaged party's use of reasonable diligence, even if the party responsible for the damages has been advised or should be aware of the possibility of such damages. In no event shall either of us be liable to the other for any punitive damages or for any loss of profits, data, revenue, business opportunities, customers, contracts, goodwill or reputation.

11. INDEMNIFICATION

11.1. You shall, at your expense, indemnify, release, hold harmless, and defend Ativion, our Affiliates, and any of our or their Representatives (the "Indemnitees") from and against any and all liability or expenses (including attorneys' and other professional fees and expenses as reasonably incurred), damages, claims, proceedings, lawsuits, threats of lawsuits, and other written allegations or claims (each, a "Claim") made or brought by a third party arising out of your actual or alleged: (i) willful misconduct; (ii) breach of applicable law; (iii) failure to meet the security obligations required by the Agreement; (iv) breach of your agreement(s) with or obligation(s) to your customers or users; (v) violation of the AUP; or (vi) your breach of Section 5 (Intellectual Property). Your obligations under this Section include Claims arising out of the acts or omissions of

your employees or agents, any other person to whom you have given access to the Services, and any person who gains access to the Services as a result of your failure to use reasonable security precautions, even if the acts or omissions of such persons were not Authorised by you.

11.2. We will choose legal counsel to defend the Claim, provided that the choice is reasonable and is communicated to you. You must comply with our reasonable requests for assistance and cooperation in the defence of the Claim. We may not settle the Claim without your consent, which may not be unreasonably withheld, delayed or conditioned.

12. NOTICES.

Your routine communications to Ativion regarding the Services should be sent to your account team using the Customer portal. To give a notice regarding termination of the Agreement for breach, indemnification, or other legal matter, you must send it by electronic mail and first-class post to:

creditcontrol@ativion.com

Accounts Receivable
Ativion
Seventh Floor, East West,
Tollhouse Hill,
Nottingham,
NG1 5FS
United Kingdom

Ativion's routine communications regarding the Services and legal notices will be sent by email or post to the individual(s) you designate as your contact(s) on your account. Notices are deemed received as of the time posted or delivered, or if that time does not fall within a Business Day, as of the beginning of the first Business Day following the time posted or delivered. For purposes of counting days for notice periods, the Business Day on which the notice is deemed received counts as the first day.

13. PUBLICITY, USE OF MARKS.

Customer agrees that Ativion may publicly disclose that it is providing Services to Customer and may use Customer's name and logo to identify Customer in promotional materials, including press releases. Customer may not issue any press release or publicity regarding the Agreement, use the Ativion name or logo or other identifying indicia, or publicly disclose that it is using the Services without Ativion's prior written consent.

14. ASSIGNMENT/SUBCONTRACTORS.

Neither party may assign the Agreement or any Orders without the prior written consent of the other party except to an Affiliate or successor as part of a corporate reorganization or a sale of some or all of its business, provided the assigning party notifies the other party of such change of control. Ativion may use its Affiliates or subcontractors to perform all or any part of the Services, but Ativion remains responsible under the Agreement for work performed by its Affiliates and subcontractors to the same extent as if Ativion performed the Services itself. Customer acknowledges and agrees that Ativion Affiliates and subcontractors may be based outside of the geographic jurisdiction in which Customer is located.

15. FORCE MAJEURE.

Neither party will be in violation of the Agreement if the failure to perform the obligation is due to an event beyond its control, such as of any fire, earthquake, flood, hurricane, tornado, snowstorm, epidemic, accident, explosion, casualty, virus or other malicious software, strike, lockout, labour controversy, riot, civil disturbance, act of public enemy, embargo, war, act of God, act of terrorism, or any municipal, county, state or national ordinance or law, or any executive, administrative or judicial order (which order is not the result of any act or omission which would constitute a default hereunder), or any failure or delay of any transportation, power, or communications system or any other or similar cause, or significant failure of a part of the power grid, failure of the Internet, or other events beyond such party's reasonable control.

16. GOVERNING LAW

16.1. The Ativion Companies. If you are contracting with Impero Solutions, Inc., then the Agreement is governed by the laws of the State of Texas, USA, exclusive of any choice of law principle that would require the application of the law of a different jurisdiction. Exclusive venue for all disputes arising out of the Agreement shall be in the state or federal courts in Travis County, Texas, and we each agree not to bring any action in any other venue. You waive all objections to this venue and agree not to dispute personal jurisdiction or venue in these courts. If you are contracting with any other of the Ativion Companies, then the Agreement is governed by the law of England and Wales and each of us expressly and unconditionally submits to the exclusive jurisdiction of the courts of England and Wales.

16.2. The Netop Companies. If you are contracting with Netop Tech, Inc., then the Agreement is governed by the laws of the State of Texas, USA, exclusive of any choice of law principle that would require the application of the law of a different jurisdiction. Exclusive venue for all disputes arising out of the Agreement shall be in the state or federal courts in Travis County, Texas, and we each agree not to bring any action in any other venue. If you are contracting with any other of the Netop Companies, then the Agreement is governed by the law of England and Wales and each of us expressly and unconditionally submits to the exclusive jurisdiction of the courts of England and Wales.

16.3. UAE Law. If Customer is based in the United Arab Emirates, in the event of a dispute arising out of or relating to this Agreement, including any question regarding its existence, validity or termination, the parties shall first seek settlement of that dispute by mediation in accordance with the Mediation Rules of the DIFC LCIA Arbitration Centre, which Rules are deemed to be incorporated by reference into this clause. If the dispute is not settled by mediation within 60 days of the commencement of the mediation, or such further period as the parties shall agree in writing, the dispute shall be referred to and finally resolved by arbitration under the Arbitration Rules of the DIFC-LCIA Arbitration Centre, which Rules are deemed to be incorporated by reference into this clause. The language to be used in the mediation and in the arbitration shall be English. The governing law of the contract shall be the substantive law of Dubai, United

Arab Emirates. In any arbitration commenced pursuant to this clause, the number of arbitrators shall be one; and the seat, or legal place, of arbitration shall be the Dubai International Financial Centre (Dubai, United Arab Emirates).

16.4. NO CLASS ACTIONS. TO THE EXTENT ALLOWED BY LAW, WE EACH WAIVE ANY RIGHT TO PURSUE DISPUTES ON A CLASS WIDE BASIS; THAT IS, TO EITHER JOIN A CLAIM WITH THE CLAIM OF ANY OTHER PERSON OR ENTITY, OR TO ASSERT A CLAIM IN A REPRESENTATIVE CAPACITY ON BEHALF OF ANYONE ELSE, IN ANY LAWSUIT, ARBITRATION, OR OTHER PROCEEDING. Each of us agrees that we will not bring a claim under the Agreement more than two years after the time that the claim accrued. The Agreement shall not be governed by the United Nations Convention on the International Sale of Goods.

17. HIPAA.

If Ativion is your Business Associate, as defined by 45 C.F.R. §160.103, then the Ativion Business Associate Agreement attached as Exhibit B applies and is incorporated herein by reference.

18. FERPA.

If Customer is an educational agency or institution to which regulations under the FERPA applies, then Ativion acknowledges that for purposes of the Services, Ativion is a "school official" with "legitimate educational interests" in the Customer Data (as those terms are defined by FERPA and its implementing regulations), and Ativion agrees to comply with the requirements of FERPA as they apply to school officials with legitimate educational interests. Customer is responsible for obtaining any parental or eligible student consent for any user's use of the Services that may be required by applicable law and to provide notification on behalf of Ativionto students (or, a student's parent, as required) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Ativion's possession as may be required under applicable law. You are responsible for addressing any records requests made by students or individuals entitled to access Customer Data subject to FERPA, provided that Ativion will provide you with commercially reasonable assistance in fulfilling such requests. You are responsible for ensuring that your annual notification of FERPA rights includes the scope of the Services and this Agreement in the definition of "school official" and "legitimate educational interest." For additional information about our practices with relation to FERPA, as well as New York State Education Law §2-d and New York Parents' Bill of Rights, please refer to our Education Privacy Notice at **www.ativion.com/legal/FERPA**, incorporated herein by reference.

19. COPPA.

If COPPA applies to the Services, you are responsible for obtaining all student and/or parental consent as required by COPPA and must provide verifiable evidence of such consent upon our written request, provided that Ativion will provide you with any reasonably requested information necessary to fulfill your obligations in obtaining consent. Where COPPA applies to Ativion as part of its provision of the Services to Customer, Ativion's information management practices are attached as Exhibit C.

20. GDPR, UK GDPR, and EUDPR

20.1. If we process “Personal Data” (also known as “Personal Information”) as defined by the Data Protection Legislation as part of delivering the Services to you, in so far as required, both you and we agree that we will comply with all applicable requirements of the Data Protection Legislation. This Section is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

20.2. You acknowledge that for the purposes of the Data Protection Legislation, we are the controller of Personal Data we use to manage our relationship with you and to allow your users to access the Services and you are the controller and Ativion is the processor of any Personal Data contained in the Customer Data (where controller and processor have the meanings as defined in the Data Protection Legislation). Where we are acting as your processor, Exhibit D sets out the scope, nature and purpose of processing by Ativion, the duration of the processing and the types of Personal Data (as defined in the Data Protection Legislation) and categories of Data Subject. Further information is contained in the Data Processing Addendum at Exhibit E.

21. DATA CONSENTS

Without prejudice to the generality of Section 20.1, you will ensure that you have all necessary appropriate consents and notices in place to enable lawful transfer of any Personal Data to Ativion for the duration and purposes of this Agreement.

22. SANCTIONS STATUS

22.1. Neither party nor any of its Affiliates or, to the best of its knowledge, any director, officer, manager, or employee of such party or any of its Affiliates is a person who (a) is the target of any laws administered by the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC") or any other governmental entity imposing economic sanctions or trade embargoes ("Economic Sanctions Laws"), or (b) is located, organised, or resident in a country or territory that is, or whose government is, the target of sanctions imposed by OFAC or any other governmental entity.

22.2. Each party shall promptly upon becoming aware thereof notify the other party if it or any of its Affiliates, or any of its or its Affiliates' directors, officers, managers, employees, or agents becomes the target of any Economic Sanctions Laws, or the country or territory where any of them is located, organized, or resident becomes the target of sanctions imposed by OFAC or any other governmental entity.

23. MISCELLANEOUS

23.1. Unless otherwise expressly permitted in the Agreement the terms of the Agreement may be varied only by a written agreement signed by both parties that expressly refers to the Agreement. An Order may be amended to modify, add, or remove Services by a formal written agreement signed by both parties or by an exchange of correspondence (including via the Ativion customer management system) that includes the express consent of an Authorised individual for each of us.The pre-printed terms of your purchase order or other business form or terms that you provide shall be void and of no effect.

23.2. If any part of the Agreement is found unenforceable, the rest of the Agreement will continue in effect, and the unenforceable part shall be reformed to the extent possible to make it enforceable and give business efficacy to the Agreement. Each party may enforce its respective rights under the Agreement even if it has waived the right or failed to enforce the same or other rights in the past. The relationship between the parties is that of independent contractors and not business partners. Neither party is the agent for the other and neither party has the right to bind the other on any agreement with a third party. The use of the word "including" means "including without limitation". Other than Representatives for the purposes of Sections 6, 7, 10, and 11, there are no third-party beneficiaries to the Agreement.

23.3. The following provisions shall survive expiration or termination of this Agreement: Defined Terms, Intellectual Property, Disclaimers, Term and Termination, Confidential Information, Limitations on Damages, Indemnification, Notices, Governing Law, HIPAA, FERPA, COPPA, GDPR, UK GDPR, EUDPR, Miscellaneous, all terms of the Agreement requiring you to pay any fees for Services provided prior to the time of expiration or termination, or requiring you to pay an early termination fee, and any other provisions that by their nature are intended to survive expiration or termination of the Agreement.

23.4. The Agreement constitutes the complete and exclusive understanding between the parties regarding its subject matter and supersedes and replaces any prior or contemporaneous representation(s), agreement(s) or understanding(s), written or oral.

23.5. Singular and Plural Terms. In the body of the ASA, both the singular and plural can be used interchangeably regardless of whether the definition refers to the singular or plural term.

EXHIBIT A
ATIVION ACCEPTABLE USE POLICY

PLEASE READ THE TERMS OF THIS POLICY CAREFULLY BEFORE USING THE SOFTWARE. This Acceptable User Policy ("AUP") governs your use, access and distribution of the products provided to you by Ativion (the "Software"), as well as any other services or activities provided to you (together, the "Services"). By using our Services, you confirm that you accept the terms of this policy and that you agree to comply with them. If you do not agree to these terms, you must not use our Services.

Who we are and how to contact us

The site www.ativion.com and its related Services are operated on behalf of the Ativion Group. The Ativion Group forms part of any and all subsidiary companies of Impala Bidco Limited, a company incorporated in England and Wales with registration number 10878303, registered at Seventh Floor, East West, Tollhouse Hill, Nottingham, NG1 5FS, consisting of Ativion Companies and Netop Companies, as identified in the Organisation Structure, available at **www.ativion.com/legal/group-structure/**

To contact us in relation to this AUP, please email **legal@ativion.com**

Prohibited Uses

You may use our Services only for lawful purposes. You may not use our Services:

- To engage in, foster or promote illegal, abusive, or irresponsible behaviour.
- In any way that breaches any applicable local, national, or international law or regulation.
- In any way that is unlawful or fraudulent or has any unlawful or fraudulent purpose or effect.
- Except to the extent that such content is educational content or is necessary for the purposes of safeguarding the wellbeing of students in a lawful manner, you may not publish, transmit, or store on or via the Services any content or links to any content that:
    - Constitutes, depicts, fosters, promotes or relates in any manner to any sexual activity.
    - Is excessively violent, incites or threatens violence, contains harassing content or hate speech.
    - Is unfair or deceptive.
    - Is defamatory or violates a person's privacy.
    - May harm or attempts to harm minors in any way.
    - Is used to bully, insult, intimidate or humiliate any person.
- To transmit, or procure the sending of, any unsolicited or unauthorised advertising or promotional material or any other form of similar solicitation (spam).
- To knowingly transmit any data, send or upload any material that contains viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar

computer code designed to adversely affect the operation of any computer software or hardware.

- To engage in any other conduct that restricts or inhibits anyone's use or enjoyment of the Services, or which, as determined by us, may harm users of the Services or expose them to liability.
- You also agree:
  - Not to attempt to probe, scan, penetrate, or test the vulnerability of an Ativion system or network, or to breach the Ativion security or authentication measures in any form (actively or passively), except to the extent expressly agreed in writing with all such testing activities made subject to a separate agreement.
  - Not to use the Services in a manner that infringes on or misappropriates the rights of a third party in any work protected by copyright, trade or service mark, invention, trade secrets, or other intellectual property or proprietary information. It is Ativion's policy to terminate a Customer contract where a Customer or its end users repeatedly infringe this in appropriate circumstances.
- Not to access without authority, interfere with, damage or disrupt:
  - any part of our Services;
  - any equipment or network on which our Services is stored;
  - any software used in the provision of our Services; or
  - any equipment or network or software owned or used by any third party

Interactive Services

We may from time to time provide interactive services on our site, including, without limitation:

- Discussion groups.
- Bulletin boards.

We will do our best to assess any possible risks for users from third parties when they use any interactive service provided on our site, and we will decide in each case whether it is appropriate to use moderation of the relevant service (including what kind of moderation to use) in the light of those risks. However, we are under no obligation to oversee, monitor or moderate any interactive service we provide on our site, and we expressly exclude our liability for any loss or damage arising from the use of any interactive service by a user in contravention of our content standards, whether the service is moderated or not.

Code of Conduct

When using the interactive services, we expect all users to comply with the following code of conduct:

- Respect others. Focus on the content of posts and not on the people making them. Please extend the benefit of the doubt to newer guests and members; there's no such thing as a stupid question.
- Respect the purpose of the community. Use the community to share successes, challenges, constructive feedback, questions, and goals instead of promoting products or services that you provide. If you've found a product or service helpful, please share your experience with the group in a respectful way.
- Use caution when discussing products. Information posted on the discussion

groups and in the libraries is available for all to see, and comments are subject to libel, slander, criminal and antitrust laws.

- All defamatory, abusive, profane, threatening, offensive, or illegal materials are strictly prohibited. Do not post anything that you would not want the world to see or that you would not want anyone to know came from you.
- Respect intellectual property. Post content that you have personally created or have permission to use and have properly attributed to the content creator.
- Post your message or documents only to the most appropriate communities. This helps ensure all messages receive the best response by eliminating "noise."

Discussion Group Etiquette

When participating in discussion groups on our site you should:

- state concisely and clearly the topic of your comments in the subject line. This allows members to respond more appropriately to your posting and makes it easier for members to search the archives by subject;
- send messages such as "thanks for the information" or "me, too" to individuals, not to the entire list. Do this by using the "Reply to Sender" link in every message; and
- not send administrative messages, such as “remove me from the list,” to the group. Instead, use the web interface to change your settings or to remove yourself from a list. If you are changing email addresses, you do not need to remove yourself from the list and rejoin under your new email address. Simply change your settings in your profile.

Content Standards

- These content standards apply to any and all material which you contribute to our site (“Contribution”) and to any interactive

services associated with it.

- The Content Standards must be complied with in spirit as well as to the letter. The standards apply to each part of any Contribution as well as to its whole.
- We will determine, in our discretion, whether a Contribution breaches the Content Standards.
- A Contribution must:
  - Be accurate (where it states facts).
  - Be genuinely held (where it states opinions).
  - Comply with the law applicable in England and Wales and in any country from which it is posted.
- A Contribution must not:
  - Be defamatory of any person.
  - Be obscene, offensive, hateful or inflammatory.
  - Bully, insult, intimidate or humiliate.
  - Promote sexually explicit material.
  - Include child sexual abuse material.
  - Promote violence.
  - Promote discrimination based on race, sex, religion, nationality, disability, sexual orientation or age.
  - Infringe any copyright, database right or trademark of any other person.
  - Be likely to deceive any person.
  - Breach any legal duty owed to a third party, such as a contractual duty or a duty of confidence.
  - Promote any illegal activity.
  - Be in contempt of court.
  - Be threatening, abuse or invade another's privacy, or cause annoyance, inconvenience or needless anxiety.

- Be likely to harass, upset, embarrass, alarm or annoy any other person.
- Impersonate any person or misrepresent your identity or affiliation with any person.
- Give the impression that the Contribution emanates from us, if this is not the case.
- Advocate, promote, incite any party to commit, or assist any unlawful or criminal act such as (by way of example only) copyright infringement or computer misuse.
- Contain a statement which you know or believe, or have reasonable grounds for believing, that members of the public to whom the statement is, or is to be, published are likely to understand as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism.
- Contain any advertising or promote any services or web links to other sites.

Breach of this Policy

- When we consider that a breach of this AUP has occurred, we may take such action as we deem appropriate.
- Failure to comply with this AUP constitutes a material breach of the terms of use upon which you are permitted to use our Services, and may result in our taking all or any of the following actions:
  - Immediate, temporary or permanent withdrawal of your right to use our Services.
  - Issue of a warning to you.
  - Legal proceedings against you for reimbursement of all costs on an indemnity basis (including, but not limited to, reasonable administrative and legal costs) resulting from the breach.
  - Further legal action against you.
  - Disclosure of such information to law enforcement authorities as we reasonably feel is necessary or as required by law.
- We exclude our liability for all action we may take in response to breaches of this acceptable use policy. The actions we may take are not limited to those described above, and we may take any other action we reasonably deem appropriate.

Which country's laws apply to any disputes?

• **USA.** If you are based in the USA, and the Customer contract is with Impero Solutions, Inc.dba Ativion or Netop Tech Inc., then the Agreement is governed by the laws of the State of Texas, USA, exclusive of any choice of law principle that would require the application of the law of a different jurisdiction. Exclusive venue for all disputes arising out of the Agreement shall be in the state or federal courts in Travis County, Texas, and we each agree not to bring any action in any other venue. You waive all objections to this venue and agree not to dispute
personal jurisdiction or venue in these courts.

• **UAE.** If Customer is based in the United Arab Emirates, in the event of a dispute arising out of or relating to this Agreement, including any question regarding its existence, validity or termination, the parties shall first seek settlement of that dispute by mediation in accordance with the Mediation Rules of the DIFC LCIA Arbitration Centre, which Rules are deemed to be incorporated

by reference into this clause. If the dispute is not settled by mediation within 60 days of the commencement of the mediation, or such further period as the parties shall agree in writing, the dispute shall be referred to and finally resolved by arbitration under the Arbitration Rules of the DIFC-LCIA Arbitration Centre, which Rules are deemed to be incorporated by reference into this clause. The language to be used in the mediation and in the arbitration shall be English. The governing law of the contract shall be the substantive law of Dubai, United Arab Emirates. In any arbitration commenced pursuant to this clause, the number of arbitrators shall be one; and the seat, or legal place, of arbitration shall be the Dubai International Financial Centre (Dubai, United Arab Emirates).

- **UK, EU, Rest of World.** If you are based anywhere else in the world and contracting with any other of the Ativion or Netop Companies, then the AUP is governed by the law of England and Wales and each of us expressly and unconditionally submits to the exclusive jurisdiction of the courts of England and Wales.

We may make changes to the terms of this policy

We may update this AUP over time as we deem necessary and appropriate in response to legal or regulatory changes, technology advances, or as we identify new forms of behaviour which pose a risk to our users, shared systems, or is inconsistent with our or our customer's legal obligations.

EXHIBIT B
BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Association Agreement ("BAA") is an addendum to your Agreement (and incorporated therein by reference). This BAA defines the rights and responsibilities of each of us with respect to Protected Health Information as defined in the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder, including the HITECH Act and Omnibus Rule, as each may be amended from time to time (collectively, "HIPAA"). This BAA shall be applicable only in the event and to the extent Ativion meets, with respect to you, the definition of a Business Associate set forth at 45 C.F.R. §160.103, or applicable successor provisions.

1. Defined Terms.

For the purposes of this BAA, capitalized terms shall have the following meanings, and otherwise as defined in the Agreement:

"Business Associate" shall generally have the same meaning as the term "business associate" at 45 C.F.R. § 160.103, and in reference to the party in this BAA, shall mean Ativion.

"Individual" shall have the same meaning as the term "individual" in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

"Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

"Protected Health Information" or **"PHI"** shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information received by Business Associate from or on behalf of Customer.

"Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

"Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

2. Obligations and Activities of Business Associate.

a) Business Associate shall not use or disclose Protected Health Information other than as permitted or required by this BAA or as permitted or Required By Law.

b) Business Associate agrees to provide those physical, technical and administrative safeguards described in the Agreement, including those safeguards and services selected by you and described in an Order. If Business Associate agrees as part of this BAA to carry out an obligation of yours under the Privacy Rule, then Business Associate will comply with the requirements of the Privacy Rule applicable to such obligation.

c) Business Associate agrees to mitigate, to the extent commercially reasonable and reasonably practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate or its agents or subcontractors in violation of the requirements of this BAA.

d) Within five Business Days of becoming aware, Business Associate agrees to report to you (i) Security Incidents (as defined in 45 C.F.R. §164.304 and as further described below), (ii) the Breach of unsecured PHI (as

defined in 45 CFR §164.402), or (iii) an access, acquisition, use or disclosure of PHI in violation of this BAA.

e) Both parties acknowledge that there are likely to be a significant number of meaningless or unsuccessful attempts to access the Services, which make a real-time reporting requirement impractical for both parties. The parties acknowledge that Business Associate's ability to report on system activity, including Security Incidents, is limited by, and to, Customer's specific Services and instances thereof, and does not include User Devices.

f) Business Associate undertakes no obligation to report unsuccessful security incidents or to report network security related incidents which occur on Ativion's managed network or systems but do not directly involve Customer Data. The parties agree that the following are illustrative examples of unsuccessful security incidents which, when they do not result in the Unauthorised access, use, disclosure, modification or destruction of PHI need not be reported by Business Associate: pings against network devices, port scans, attempts to log on to a system or database with an invalid password or username, malware.

g) Business Associate agrees to obtain from any agent, including a subcontractor to whom it provides Protected Health Information, reasonable assurances that it will adhere to the same restrictions and conditions that apply to Business Associate under this BAA with respect to such information.

h) All Protected Health Information maintained by Business Associate for you will be available to you in a time and manner that reasonably allows you to comply with the requirements under 45 CFR § 164.524. Business Associate shall not be obligated to provide any such information directly to any Individual or person other than you.

i) All Protected Health Information and other information maintained by Business Associate for you will be available to you in a time and manner that reasonably allows you to comply with the requirements under 45 CFR § 164.526.

j) Business Associate agrees to make internal practices, books, and records available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary's determining your compliance with the Privacy Rule; provided, however, that time incurred by Business Associate in complying with any such request that exceeds its normal customer service parameters shall be charged to you at Business Associate's then current hourly rate for additional services.

k) You acknowledge that Business Associate is not required by this BAA to make disclosures of Protected Health Information to Individuals or any person other than you, and that Business Associate does not, therefore, expect to maintain documentation of such disclosure as described in 45 CFR § 164.528. In the event that Business Associate does make such disclosure, it shall document the disclosure as would be required for you to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR §164.504(e)(2)(ii)(G) and §164.528 and shall provide such documentation to you promptly on your request. In the event that a request for an accounting is made directly to Business Associate, Business Associate shall, within 2 Business Days, forward such request to Customer.

3. Permitted Uses and Disclosures by Business Associate.

Except as otherwise limited by this BAA or other portion of the Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or Services for, or on behalf of, you as specified in the Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by you.

4. Specific Use and Disclosure Provisions.

Except as otherwise limited in this BAA or other portion of the Agreement, Business Associate may:

a)use Protected Health Information for the proper management and administration of Business Associate or to carry out its legal responsibilities;

b) disclose Protected Health Information for the proper management and administration of Business Associate, provided that disclosures are (i) Required By Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person will notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached; and

c) use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1).

5. Your Obligations.

You shall notify Business Associate of:

a) any limitations(s) in your notice of privacy practices in accordance with 45 CFR § 164.520 to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information;

b) any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information; and

c) any restriction to the use or disclosure of Protected Health Information that you have agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information. You agree that you will not request that Business Associate use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by you. You agree to comply with those security obligations identified in the Agreement, and to implement or maintain appropriate safeguards and practices as required for you to comply with the Security and Privacy Rules as applicable to you.

6. Term and Termination

a) The term of this BAA shall continue for the term of the Agreement to which this BAA is incorporated by reference, and following termination of such Agreement until all Protected Health Information is destroyed or returned to you or your designee.

b) If Business Associate materially breaches the terms of this BAA, then you may terminate any related Agreements(s).

c) Upon termination of the Agreement for any reason Business Associate shall destroy all Protected Health Information which remains on the Ativion Platform or otherwise

in Business Associates possession. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate as well as Business Associate itself. Business Associate shall retain no copies of the Protected Health Information. In the event that Business Associate determines that destroying the Protected Health Information is infeasible, Business Associate shall promptly provide you notification of the conditions that make destruction infeasible. Business Associate shall extend the protections of this BAA to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the destruction infeasible, for so long as Business Associate maintains such Protected Health Information. You shall bear the cost of storage of such Protected Health Information for as long as storage by Business Associate is required. This Section does not require Business Associate to segregate any Protected Health Information from other information maintained by you on Business Associate's servers and Business Associate may comply with this requirement by deleting all of the Protected Health Information received from you and maintained on the Ativion Platform or Business Associate's systems.

d) If you request contemporaneously with any termination event or notice, Business Associate will allow you to have access to your Customer Data a reasonable period of time following termination as necessary for you to retrieve or delete any Protected Health Information at your then current fees; provided, however, that if the Agreement was terminated for your breach of the AUP or the Agreement, Ativion may: (i) provide you with restricted access via a private link to your Customer Data or (ii) use reasonable efforts to copy your data on to media you provide to Ativion, and will ship the media to you at your expense. Ativion's efforts to copy your data onto your media shall be billable at Ativion's then current hourly rates.

7. Miscellaneous.

7.1. Amendment. Each of us agrees to take such action as is reasonably necessary to amend this BAA from time to time as is necessary for you to comply with the requirements of HIPAA as they may be amended from time to time; provided, however, that if such an amendment would materially increase the cost of Business Associate providing service under the Agreement, Business Associate shall have the option to terminate the Agreement on thirty (30) days advance notice. Any ambiguity in this BAA shall be resolved to permit you to comply with HIPAA and the Privacy Rule.

7.2. Survival. Our respective rights and obligations under this BAA shall survive the termination of the Agreement.

EXHIBIT C
NOTICE OF COPPA PRACTICES

Last Updated and Effective: September 20, 2024

Impero Solutions, Inc. dba Ativion and Netop Tech Inc. affiliates ("Ativion") provides its customer educational institutions ("Schools") with cloud-based services which enable the Schools to administer their systems, student systems, track student progress and welfare concerns, enhance School staff collaboration, and organize student information (the "Services"). Consistent with our obligations under Children's Online Privacy Protection Act ("COPPA"), we provide this Notice of COPPA Practices (this "Notice") to better assist Schools, students, parents, and teachers in understanding how we receive, store, and manage the information we collect in the Services. Ativion is required by COPPA to provide the following information, which Schools may also provide to their students and parents in order to effectively inform the consent requirements under laws applicable to the School.

For more information about COPPA and general tips about protecting Children's online privacy, please visit the Federal Trade Commission's website at: **https://www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online.**

Ativion relies on Schools to obtain consent from parents for the collection and use of personal information of students (of any age), in compliance with FERPA and their local legal and policy requirements. The remaining section is the notice as it may be disclosed to the students and parents.

Ativion Children's Privacy Notice

Impero Solutions, Inc. dba Ativion or Netop Tech Inc. (collectively, "Ativion"), understands the importance of personal information and privacy of children. This Ativion Children's Privacy Notice ("Notice") describes additional details about how Ativion will collect, use, access, store, disclose, and otherwise process personal information from an individual under the age of 13 ("Child" or "Children"). In this Notice, "Service" means Ativion's EdLink, Webcheck, Wellbeing, Classroom, Education Pro, Backdrop, ContentKeeper and other related services (collectively, "Services"). Ativion makes use of the personal information collected in order to provide the Services to school where the child attends ("Schools") as agreed in their given Orders, and for no other commercial purpose.

1. Information Ativion Collects from Children.

Ativion collects and maintains any personal information of Children received through the Services. Below are instances where we may receive Children's personal information from the Schools and how we will provide parents/guardians with notice and seek verifiable parental consent. If we learn that we have collected or received personal information from a child without verifiable consent from a parent or guardian, we will delete that information and seek parental consent. The information collected by Ativion varies by product and by School based on the specific implementation and selected usage.

- **Contact Information.** To participate in our Services, we ask children and their parent(s) or guardian(s) to set up an account through your School.
- **Account Information.** We may collect the child's name, gender, grade level, account username, password. We will also require the child to provide the parent or guardian's email address for notifications to be sent from our Services.
- **Wellness Information.** keyword detection and monitoring, online activity logging, context capture (screenshot/video recording), self-submitted student information about their wellness.
- **Geolocation Information.** We collect the geolocation information when a Child accesses our Services to provide the correct language and time zone for our Services.
- **Activity and Usage Information.** We collect children's Service usage information to identify inappropriate behaviour or activities, Service utilization rates, internet usage, and
- technical issues.
- **Course Participation and Testing Information.** Some of our Services will collect the child's name and identity, test scores, curriculum completion, active viewing of current device usage, messaging and live chat content. Monitoring of devices and usage to identify restricted use or inappropriate behaviour.
- **Communication Information.** Some of our Services require teachers to communicate directly with the children enrolled in classes through communication tools. Our personnel are trained to avoid discussing or collecting personal information from Users and engaging in inappropriate communications.
- **Student Profile Information.** Some of our Services, such as Backdrop will use personal information to create a student profile that will include demographic information, welfare history, medical history, sibling identity, home address, persistent identifiers, student images.
- **Device Information.** We collect information about the user's devices including last known IP address, hardware system information (PC or Macintosh), operating system, and web browser information, and system preferences which includes language and accessibility settings.

Ativion notes that Children cannot make their information publicly available, although they can provide information to teachers and the School using the Services.

2. Reasons for collecting and using children's information

Ativion uses the collected personal information solely for the purposes of providing the websites and Services to the School, in accordance with the agreement with the School, applicable law, our Privacy Policy and all related privacy notices available at **www.ativion.com/legal/privacy-policy**

3. Who Do We Disclose or Share Information.

Ativion may share or disclose personal information collected from children with the following categories of entities for the following reasons:

- **Schools.** We will disclose children's personal information to the Schools for the purposes outlined in "Reasons for collecting and using children's information."
- **Affiliates.** We may share children's personal information to our affiliates to provide the child and Schools with our Services.
- **Suppliers and Service Providers.** Ativion may utilize subcontractors and its Affiliates to assist it in the delivery of the Services, including for purposes of storing personal information received through the websites and Services. As of the date of this Notice, Ativion utilizes Microsoft's Azure Cloud to host elements of the websites and Services.
- **Government authorities and law enforcement agencies.** We may be required to provide information: (1) as required by law, (2) based on government agency requests, or (3) upon request by valid legal process, such as subpoenas or court orders, issued by a court of competent jurisdiction.

4. Parental Choices and Controls.

Ativion handles all requests relating to its provision of the Services. Schools, parents or guardians may review the information we have collected from their children, refuse to permit further collection of personal information from their child, and request the deletion of the collection information. If you are a parent and have concerns, we suggest that you contact your child's School or teacher so that they can respond directly to your concerns. Ativion will respond to any inquiries from a School directed to: support@ativion.com. Please note that request, change or deletion of personal information on an account may result in the termination of your child's account with our Service. Ativion may engage in validation procedures, including relaying your request to the School, in order to protect collected information from Unauthorised disclosure or deletion.

For more information, see our Education Privacy Notice found at: **www.ativion.com/legal/FERPA/**.

5. Frequently Asked Questions.

- **Does Ativion Use or Share the Information for Commercial Purposes Not Related to the Provision of the Services Requested by the Customer?** No. Ativion only collects and uses personal information collected from students for the use and benefit of the School and for no other purpose. This enables Schools to obtain consent directly from parents. We require that Schools provide administrative contacts Authorised to consent on behalf of

parents and implement identity management controls to ensure that the School officials are providing the consent (and not a student pretending to be a teacher, for example).

- **Does Ativion Enable the School to Review and Have Deleted the Personal Information Collected From Their Students?** Yes. Schools remain directly in control of the majority of information collected by the Services and are the primary administrator of such data. Where Ativion's Services also collect usage data or similar analytics which are presented to the School, Ativion will provide will delete such information upon the School's request, which may necessitate termination of the Services.
- **What Measures Does Ativion Take to Protect the Security, Confidentiality, and Integrity of the Personal Data that it Collects?** Ativion implements administrative, technical, and physical access controls designed to protect the security, confidentiality, and integrity of the Personal Data (as defined by the GDPR) it collects at the locations in which such data or systems are stored. As a global provider of educational technology services and solutions, Ativion takes data security and privacy seriously and complies with the EU General Data Protection Regulation (the "GDPR") where applicable. The controls required to comply with the GDPR are implemented throughout Ativion's service delivery model. For more information please see the UK-EU GDPR Notice: **www.ativion.com/legal/GDPR/**. For student records, we abide by the Family Educational Rights and Privacy Act (FERPA) and state education laws concerning student records. For more information regarding student records and parent's bill of rights to student records, please review our Education Privacy Policy at **www.ativion.com/legal/FERPA/**.

EXHIBIT D
Details of the Processing

Nature and scope of processing	All processing activities required in relation to the performance of the Services under the Agreement.
Purpose of processing	Personal Data will be processed during the term of the ADA, including any data processing for transition and termination assistance. Personal Data will be deleted or returned by Ativion to Schools thereafter. provision of the Services to you.
Duration of processing	The duration of the provision of the Services to you.
Data Subjects	Individuals whose Personal Data is included in Customer Data, include the following: [For Ativion's EdLink, Webcheck, Wellbeing, Classroom, Education Pro, Backdrop, ContentKeeper offerings] Students Teachers Administrators Parents/Guardians [For Netop service offerings] Customer Employees Customer Contractors Customer representatives
Categories of Personal Data	Categories of Personal Data processed will depend on the Service offerings selected: [For Ativion's EdLink, Webcheck, Wellbeing, Classroom, Education Pro, Backdrop, ContentKeeper offerings] Name (First, middle, last), Email address, Phone number, User login/password Account information (preferences), Student ID, Educational information, Imprecise Geolocation, Behavioural information, Medical information, Wellness information, Service usage information, Communications information, Device information (IP address, hardware, software, operating system information) [For Netop service offerings] Name (First, middle, last), Email address, Phone number, User login/password Account information (preferences), Service usage information, Device information (IP address, hardware, software, operating system information)

EXHIBIT E
DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedules and Appendices ("DPA") forms part of the ASA ("Agreement") or other written or electronic agreement between Ativion and Customer. By signing the Agreement, Customer enters into this DPA on behalf of itself and its Authorized Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorised Affiliates.

All capitalized terms not defined in the DPA shall have the same meaning as those defined in the Agreement, including any Schedules or Appendices. In the course of providing the Services to Customer pursuant to the DPA, Ativion may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith. This DPA supplements the data privacy and security obligations of each Party.

1. DEFINITIONS

"Authorised Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws and Regulations, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Ativion, but has not signed its own Order with Ativion and is not a "Customer" as defined under this DPA.

"CCPA" means shall have the same meaning as defined by the Agreement.

"Data Protection Laws and Regulations" shall have the same meaning as defined by the Agreement.

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

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

"Processor" means the legal person which Processes Personal Data on behalf of the Controller, or as the term is defined in the applicable Data Protection Laws and Regulations.

"Security Incident" means the actual unauthorized disclosure, acquisition of, or access to, the Personal Data that does or may compromise the security, confidentiality and/or integrity of the Personal Data.

"Sub-processor" means any Processor engaged by Ativion or a member of the Ativion Group.

The terms **"Business", "Personal Information", "Sell", "Share",** and **"Service Provider"** shall have the same meaning as the terms defined in the CCPA.

2. PROCESSING OF PERSONAL DATA

2.1. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and Business and Ativion is the Processor and Service Provider, as such terms are defined in the applicable Data Protection Laws and Regulations. Ativion will treat the Personal Information as the Confidential Information of Client. Ativion or members of Ativion Group will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2. Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of Ativion as Processor and obtaining consents. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3. Details of the Processing. The subject matter, duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are specified in Exhibit D (Details of the Processing) to this DPA.

2.4. General Provisions. As a Processor Customer's Personal Data, Ativion shall:

- (a) process Personal Data only on Customer's written instructions (provided that such instructions are within the scope of the Services set out in the Agreement) unless Ativion is required by applicable Data Protections Laws and Regulation to process Personal Data. When such applicable Data Protections Laws and Regulations require processing of Personal Data outside of the scope of Customer's instructions, Ativion will promptly notify the Customer of this before performing the processing required by the applicable laws unless those applicable laws prohibit Ativion from doing so.
- (b) ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational

measures adopted by it).

- (c) ensure that all Ativion personnel who have access to and/or process Personal Data are subject to the duty of confidentiality, contractually or statutorily, to keep the Personal Data confidential.
- (d) not transfer any Personal Data outside of the applicable geographic area without ensuring adequate measures are in place to protect the Personal Data as required by applicable Data Protection Laws and Regulation.
- (e) reasonably assist Customer in ensuring compliance with the obligations under the Data Protection Laws and Regulations, as applicable, considering the nature of Processing and the information available to Ativion, upon Customer's reasonable request.
- (f) maintain records of processing categories of activities carried out on behalf of the Customer.
- (g)notify Customer if Ativion believes any Processing required under the Agreement is contrary to Customer's instructions or what is allowed under the applicable Data Protection Laws and Regulations.
- (h)notify Customer if Ativion determines that it can no longer meet its obligations under applicable Data Protection Laws and Regulations.

3. DATA SUBJECT REQUEST.

Ativion shall, to the extent legally permitted, promptly notify Customer if Ativion receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Taking into account the nature of the Processing, Ativion shall assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer does not have the ability to address a Data Subject Request, Ativion shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Ativion is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. Customer shall be responsible for any costs arising from Ativion's provision of such assistance.

4. ATIVION PERSONNEL

4.1. Training and Confidentiality. Ativion shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate recurring training on their responsibilities and have executed written confidentiality agreements. Ativion shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.3. Limitation of Access. Ativion shall ensure that access to Personal Data is determined on a principle of least privilege and limited to those personnel performing Services in accordance with the Agreement.

4.4. Data Protection Officer. The Ativion Group has appointed a data protection

officer. The data protection officer can be contacted on **dpo@ativion.com**.

5. SUB-PROCESSORS

5.1. Appointment of Sub-processors. Customer acknowledges and agrees that it provides general authorization to Ativion to engage Sub-processors. Specifically, Customer acknowledges that (a) Ativion's Affiliates may be retained as Sub-processors; and (b) Ativion Group may engage third-party Sub-processors in connection with the provision of the Services. When engaging a Sub-processor, Ativion Group will enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPAto the extent applicable to the nature of the Services provided by such Sub-processor, including that the Sub-processor will provide sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of applicable Data Protection Laws and Regulations.

5.2. List of Current Sub-processors. Ativion shall make available to Customer, on Ativion's website, the current list of Sub-processors used, and their country of location. The current list of Ativion Sub-processors may be found at: **www.ativion.com/legal/sub-processor/**

5.3. Objection. Before engaging a new Sub-processor, Ativion will notify Customer with details of the new Sub-processor through an update to its website at **www.ativion.com/legal/sub-processor/** or notification to the Customer via email at least thirty (30) days before engaging the Sub-processor. Customer may object to Ativion's use of a new Sub-processor by notifying Ativion promptly in writing within ten (10) days after receipt of Ativion's notice, which must be based on reasonable grounds relating to Data Protection Laws and Regulations. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Ativion will use reasonable efforts to cooperate with the Customer to make commercially reasonable changes to Customer's configuration or use of the Services to accommodate the Customer's objection. If Ativion cannot accommodate the Customer's objection, the parties shall come together in good faith to discuss a resolution to the objection. Such discussions shall not affect Ativion's right to use the new Sub-processor after the thirty (30) day period.

5.4. Liability. Ativion will remain liable to the Customer for ensuring Sub-processors' compliance with its data protection obligations.

6. SECURITY

6.1. Controls for the Protection of Customer Data. Ativion shall maintain appropriate technical and organisational measures for protection of the security (including protection against unauthorised or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorised disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data. Ativion regularly monitors compliance with these measures. Customer acknowledges that the security measures are subject to technical progress and development and that Ativion may update or modify its technical and organizational measures from time to time, provided that Ativion will not materially decrease the overall security of the Services during a subscription term.

6.2. Data Protection Impact Assessment. Upon Customer's request, Ativion shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information and such information is available to Ativion.

7. INCIDENT MANAGEMENT AND NOTIFICATION.

7.1. Within seventy-two (72) hours of a Security Incident first becoming known to Ativion, Ativion will notify Customer by email to the most recent email address provided by Customer to Ativion. The email shall contain a summary of all facts then known about the Security Incident.

7.2 To the extent reasonably necessary, at Ativion's discretion, Ativion will provide Customer with a more-detailed notification than that required by Section 7.1, again to the most recent email address, containing at least the following information, to the extent such information is available to Ativion upon reasonable investigation:

- (i) the identification and address of each Data Subject impacted by the Security Incident;
- (ii) a brief description of what happened, including, without limitation, the date of the Security Incident and the date of the discovery of the Security Incident;
- (iii) a description of the types of Personal Data that were involved in the Security Incident;
- (iv) a detailed list of all steps that impacted Data Subjects should take to protect themselves from potential harm that will or may result from the Security Incident;
- (v) a brief description of what Ativion is doing to investigate the Security Incident, mitigate the harm to Data Subjects, and protect against further Security Incidents;
- (vi) a brief description of what Ativion plans to do in the immediate future to further investigate the Security Incident, mitigate the harm to Data Subjects, and protect against further Security Incident; and
- (vii) complete contact information for a management-level person at Ativion for further communications with Customer regarding the Security Incident.

7.3 Upon Customer request, Ativion will promptly notify Customer via email with updates of the items specified in Section 7.2.

7.4 Unless required by applicable Data Protection Laws and Regulations, and then only to the extent so required, Ativion will not inform any third party, including, without limitation, any impacted Data Subjects, of any Security Incident without first obtaining the prior express and unambiguous consent of Customer. Ativion acknowledges and agrees that Customer has and will have the sole right to determine: (i) whether to provide notice of any Security Incident to any of the Data Subjects, as required by law or regulation or in Customer's discretion, including, without limitation, the contents and delivery method thereof; and (ii) whether to offer any type of remedy, and the nature and extent of any such remedy, to Data Subjects.

8. RETURN AND DELETION OF CUSTOMER DATA.

Upon Customer request, Ativion shall return Customer Data in Ativion's possession to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the ASA and applicable privacy policies (available at http://www.ativion.com/legal/), unless retention of such Customer Data is required by applicable law.

9. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorised Affiliates and Ativion, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, Ativion's and its Affiliates' total liability for all claims from Customer and all of its Authorised Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorised Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorised Affiliate that is a contractual party to any such DPA.

10. EUROPEAN SPECIFIC PROVISIONS

10.1 Standard Contractual Clauses. If Ativion or its Authorized Affiliates or Sub-processors, receives, collects, uses, stores or in any other way processes Personal Data of individuals residing in the UK or the European Economic Area as a result of the Services provided under the ASA, and Ativion receives, collects, uses, accesses, or transfers or in any other way Processes such Personal Data outside of the UK, the European Economic Area, or a country that has received an adequacy decision from the European Commission, Ativion and each applicable Authorized Affiliates and subcontractor will execute the appropriate Standard Contractual Clauses and/or international data transfer agreements ("IDTA"), as applicable, with all applicable parties, including Customer, if necessary.

10.2 Options for EU Standard Contractual Clauses. To the extent parties execute the Standard Contractual Clauses set forth in Schedule 2, the following term options shall apply:

- Clause 7 (Optional docking clause) iS applicable;
- Clause 9 (Use of sub-processors) option 2 shall apply and the specified time or period to notice the change in sub-processor shall be set forth in Section 5 of this DPA;
- Clause 11(a) (Redress) shall not be applicable;
- Clause 17 (Governing law) option 2 shall apply, and the Parties agree that the EU Member States law shall be the law of Denmark; and
- Clause 18 (Choice of forum and jurisdiction) the Parties agree that the courts of Denmark shall have jurisdiction.

10.3 Options for UK International Data Transfer Agreements. In case of any transfers of Personal Data under this DPA

under the Standard Contractual Clauses from the United Kingdom, to the extent such transfers are subject to Data Protection Laws and Regulations applicable in the United Kingdom the parties will agree to the terms set of the IDTA in Schedule 3.

11. U.S. STATE PRIVACY LAW SPECIFIC PROVISIONS

11.1 Ativion agrees that it will only Process the Personal Data for the limited and specific business purpose contemplated in the ASA, statement of work and any subsequent agreements, namely, the provision of the Services.

11.2 Ativion further agrees:

- a. It shall comply with all applicable obligations under California Privacy Law and provide the same level of privacy protections as required by California Privacy Law.
- b. Customer has the right to take reasonable and appropriate steps to ensure that Ativion uses the Personal Data in a manner consistent with Customer's obligations under California Privacy Law.
- c. It shall notify Customer if Ativion determines that it can no longer meet its obligations under California Privacy Law.
- d. Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer's Personal Data.
- e. Ativion will cooperate with Customer in responding to and complying with consumer requests, and Ativion will provide Customer with information necessary for Customer to comply with the requests. Alternatively, Ativion may enable Customer through its technology to comply with the requests.

11.3 Ativion agrees that it shall not:

- a. Sell or share the Personal Data;
- b. Retain, use, or disclose the Personal Data for any purpose other than the business purpose, namely for the provision of Services;
- c. Retain, use, or disclose the Personal Data for any commercial purpose other than the business purpose;
- d. Data Information outside the direct business relationship between Ativion and Customer; and
- e. Combine Personal Data with personal data that Ativion receives from, or on behalf of has or receives on behalf, another person or persons, or collects from its own interaction with an individual, unless it is permitted by applicable California Privacy Law.

12. AUDIT.

Ativion will adopt and maintain policies to demonstrate compliance with this DPA and the Data Protection Laws and Regulations. No more than once every twelve (12) months, or upon reasonable request by Customer after a Security Incident or request by supervisory authority, Ativion will allow and cooperate with a reasonable audit and inspection by Customer. In the alternative, Ativion may arrange for a qualified and independent auditor to conduct an audit and inspection of Ativion's compliance which audit shall use an appropriate and accepted control standard or framework/procedure. The audit shall take place during normal business hours, subject to reasonable confidentiality obligations, and in a manner that does not unreasonably disrupt the other Party's business operation, at Customer's cost. Ativion shall provide a report of such

audit to Customer upon Customer's request.

13. AMENDMENTS.

Parties agree that they will discuss in good faith to negotiate amendment of this DPA to comply with model contracts, agreements, contractual terms and conditions to address changes in applicable Data Protection Laws and Regulations.

14. CONFLICTS.

In the event of any conflicts between this DPA and the Agreement (except for Exhibits B and C), and any obligations in any applicable Order, the terms of this DPA shall prevail. Notwithstanding the foregoing, if there are any conflicts between the terms of Exhibits B or C, and this DPA, the terms of Exhibits B and C shall prevail. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses in Schedule 3, the Standard Contractual Clauses/IDTA shall prevail.

List of Schedules of this DPA

- Schedule 1: Transfer Mechanisms for European Data Transfers
- Schedule 2: Standard Contractual Clauses
- Schedule 3: International Data Transfer Agreement (UK ICO's Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018)
-

EXHIBIT E, SCHEDULE 3
STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

- (b) The Parties:
  - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
- (iii) Clause 9(a), (c), (d) and (e);
- (iv) Clause 12(a), (d) and (f);
- (v) Clause 13;
- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e); and
- (viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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.

MODULE TWO: Transfer controller to processor

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 content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

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

8.5 Duration of processing and erasure or return of data. Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data

importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

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

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

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

account the nature of processing and the information available to the data importer.

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

8.8 Onward transfers The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union2 (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

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

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

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

(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,

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

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

MODULE TWO: Transfer controller to processor

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 thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
(f) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(g) 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.
(h) 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.
(i) 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

MODULE TWO: Transfer controller to processor

(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

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

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.

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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.

(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

MODULE TWO: Transfer controller to processor

(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;[4]
- (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

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

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

MODULE TWO: Transfer controller to processor

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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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 [for Module Three: and the controller] 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 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

MODULE TWO: Transfer controller to processor

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

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

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

(b) The Parties agree that those shall be the courts of Denmark.

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

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

APPENDIX

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

ANNEX I
A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

- Name: … As set forth in ASA
- Address: … As set forth in the ASA
- Contact person's name, position and contact details: … As set forth in the signature line of ASA
- Activities relevant to the data transferred under these Clauses: … See Exhibit D
- Signature and date: … As set forth in the signature line of ASA
- Role (controller/processor): controller

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

- 1. Name: …As set forth in ASA
- Address: …As set forth in ASA
- Contact person's name, position and contact details: …As set forth in the signature line of ASA
- Activities relevant to the data transferred under these Clauses: See Exhibit D
- Signature and date: … As set forth in the signature line of ASA
- Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred
See Exhibit D.

Categories of personal data transferred
See Exhibit D.

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

The personal data transferred concern the following special categories of data (please specify):
Data exporter may submit special categories of data to the SCC Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

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

Nature of the processing
See Exhibit D.

Purpose(s) of the data transfer and further processing
See Exhibit D.

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

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

C. COMPETENT SUPERVISORY AUTHORITY

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

- [OPTION 1: If EEA Customer, Customer location]
- [OPTION 2: if UK Customer, UK ICO]
- [OPTION3: U.S. Customer Denmark Data Protection Authority]

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the SCC Services, as described in the Security, Privacy and Architecture Documentation applicable to the specific SCC Services purchased by data exporter, and accessible via email to **support@ativion.com** or otherwise made reasonably available by data importer. The data importer will not materially decrease the overall security of the SCC Services during a subscription term.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

For the list of Ativion's Sub-Processors, please access:
http://www.ativion.com/legal/sub-processor

Standard Data Protection Clauses to be issued by the Commissioner under S119A (1) Data Protection Act 2018 International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

Table 1: Parties

The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' detail	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Impero Solutions, Ltd. Trading name (if different): Ativion Main address (if a company registered address): Unit 306, 70 Wapping Wall, London E1W 3SS, UK Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Asta Kill Job Title: DPO Contact details including email: dpo@imperosoftware.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	þ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

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

Annex 1A: List of Parties: See EU SCCs

Annex 1B: Description of Transfer: See EU SCCs

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See EU SCCs

Annex III: List of Sub processors (Modules 2 and 3 only): See EU SCC

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: • Importer • Exporter þ neither Part

Part 2: Mandatory Clauses

Entering into this Addendum

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

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

UK GDPR	As defined in section 3 of the Data Protection Act 2018.

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

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

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies

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

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

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

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

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

- a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that

data transfer, and they provide Appropriate Safeguards for those data transfers;

- b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
- c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

- a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
- b. In Clause 2, delete the words:
  - "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
- c. Clause 6 (Description of the transfer(s)) is replaced with:
  - "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
- d. Clause 8.7(i) of Module 1 is replaced with:
  - "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
- e. Clause 8.8(i) of Modules 2 and 3 is replaced with:
  - "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
- f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
- g. References to Regulation (EU) 2018/1725 are removed;
- h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
- i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

- j. Clause 13(a) and Part C of Annex I are not used;
- k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
- l. In Clause 16(e), subsection (i) is replaced with:
  - "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";
- m. Clause 17 is replaced with:
  - "These Clauses are governed by the laws of England and Wales.";
- n. Clause 18 is replaced with:
  - "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and
- o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

- 16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
- 17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 18. From time to time, the ICO may issue a revised Approved Addendum which:
  - a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
  - b. reflects changes to UK Data Protection Laws;

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

- 19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
  - a. its direct costs of performing its obligations under the Addendum; and/or
  - b. its risk under the Addendum,

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

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

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.