Machine Safety Design Hub Terms of Service

Table of Contents

OMRON Corporation (the "**Company**") has established these Terms of Service ("**these Terms**") governing the use of the "Machine Safety Design Hub Service" (the "**Service**") provided by the Company. The provision of the Service is subject to compliance with these Terms by the Customer and User(s) of the Service. By using the Service, the Customer and each User shall be deemed to have fully understood and agreed to these Terms and the Service Description for the Machine Safety Design Hub prepared by the Company (the "**Service Description**").

Article 1 (Application of Terms of Service)

1. These Terms shall apply to all aspects of the Customer's access and use of the Service, including the access to it and its use by Users (as defined in section 2 of these Terms).
2. The acceptance of these Terms constitute the formation of a contract between the Customer (as defined in section 2 of these Terms) and the Company.
3. By accepting these Terms, or by creating a customer account you represent and warrant that: (i) you, as User, are acting on behalf of a legal entity (identified as Customer according to the definition in section 2 of these Terms), either as an employee with sufficient authority or under application of a power of attorney; (ii) you have full legal authority to bind your employer or such entity to these Terms; (iii) you have read and understood these Terms.
4. All rules and regulations, including the Service Description, that the Company may provide to the Customer from time to time shall constitute an integral part of these Terms, regardless of their title, and the Customer agrees to be bound by them. Furthermore, the terms of the EU Data Act Addendum are incorporated in these Terms, if the EU Data Act (Regulation (EU) 2023/2854) applies to the provision of the Services to the Customer.
5. In the event of any conflict between these Terms and the provisions of an individual Customer Agreement (as defined in Article 2) between the Company and the Customer, the individual Customer Agreement shall prevail.

Article 2 (Definitions)

1. In these Terms, the following terms shall have the respective meanings set forth below.
   (1) "**Service**"
   The service provided by the Company to the Customer as the "Machine Safety Design Hub Service," consisting of the basic operations and functions, implementation and operational support, and other optional features specified in these Terms and the Service Description.
   (2) "**User Manual**"
   The manuals provided by the Company to the User regarding the Service, including procedure manuals, operation manuals, overview documents, and other materials for using the Service.
   (3) "**Customer Agreement**"

An individual contract entered into between the Company and the Customer regarding the provision and use of the Service, subject to the terms of this document.

(4) "**Service Equipment**"

Computers, servers, telecommunications equipment, and other devices and software installed or managed by the Company for providing the Service.

(5) **"Customer Equipment**"

Computers, servers, telecommunications equipment, filming/recording devices, and other devices and software installed or managed by the Customer for using the Service.

(6) "**Customer Data**"

All data, text, images, videos, audio, programs, graphics, design drawings, blueprints, specifications, Service access logs, Service operation logs, search information, IP addresses, dates, referring/exit pages, information regarding the Customer's use of the Service and communications, and all other information provided by the Customer to the Company via upload through the Customer Equipment or other methods for the purpose of using the Service or in connection with the use of the Service.

(8) **"User"**

A natural person who accesses and uses the Service on behalf of and under the responsibility of the Customer and under a license purchased by the Customer. User status is reserved to employes, officers, agents, contractors or other individuals affiliated with the Customer.

(9) "**User ID**"

A code used to identify the User from other persons.

(10) "**Password**"

A code used in combination with the User ID to identify the User from other persons.

(11) **"Customer"**

The legal entity entering into this Customer Agreement.

(12) **"Authorized Agent"**

A sales agent or control equipment distributor designated by the Company to sell the Service.

(13) **"The Company"**

OMRON Corporation Ltd, with registered address at […].

Article 3 (Formation of Customer Agreement)

1. A Customer Agreement for the Service shall be formed when the Customer applies for use of the Service in accordance with the application procedures prescribed by the Company, and the Company sends notice of acceptance by the method prescribed by the Company.
2. In addition to the preceding paragraph, the Customer may apply for use of the Service through an Authorized Agent. In such case as well, the Customer Agreement shall be formed between the Customer and the Company.
3. The Customer shall apply for use of the Service pursuant to the preceding two paragraphs after agreeing to these Terms. When the Customer submits such application, the Company

shall deem that the Customer has read and agreed to these Terms.

4. Any amendment to a Customer Agreement (including additions or deletions of licenses) shall be formed when the Customer applies for such amendment in accordance with the amendment application procedures prescribed by the Company, and the Company sends notice of acceptance by the method prescribed by the Company.
5. Notwithstanding the provisions of the preceding paragraphs and other provisions of these Terms, the Company may refuse to accept an application for use of the Service or any amendment to a Customer Agreement if the Customer falls under any of the following:
   (1) The Customer Agreement has been previously terminated due to the Customer's default of monetary obligations or other breach of the Customer Agreement, etc.;
   (2) The application for use of the Service or any amendment to a Customer Agreement contains false statements, errors, or omissions;
   (3) The Customer has failed, or is likely to fail, to perform its monetary obligations to the Company or other obligations under the Customer Agreement, etc.; or
   (4) The Company otherwise deems it inappropriate to accept the application under legal and reasonable grounds.

Article 4 (Amendment of Terms of Service)

1. The Company may amend these Terms or the Service Description at any time when it deems it necessary due to the enactment, amendment or abolition of laws and regulations, changes in the content or conditions of the provision of the Service, or other legitimate business reasons. In such case, the conditions for use of the Service and other contents of the Customer Agreement applied to the Customer shall be governed by the amended Terms or Service Description upon its notification to Customer according to the following numeral.
2. In the case of the preceding paragraph, the Company shall notify the Customer of the amended Terms or Service Description by any of the following methods:
   (1) By email to the email address registered by the Customer.
   In this case, notification shall be deemed to have been made when the email sent by the Company is recorded on the email server of the email address registered by the Customer (regardless of whether the Customer actually reads said email).
   (2) By posting on the Company's designated website for the Service.
   In this case, notification shall be deemed to have been made when these Terms or the Service Description posted on the website become available for viewing by the Customer (regardless of whether the Customer actually views the website).
   (3) By posting on the Service portal site.
   In this case, notification shall be deemed to have been made when these Terms or the Service Description posted on the portal site become available for viewing by the Customer (regardless of whether the Customer actually views the portal site).
   (4). Customer's right to terminate.- If the amendment to these Terms or the Description of the

Service is not implemented by Company as a result of the enactment, amendment or abolition of laws and regulations and such amendment to these Terms or the Description of the Service materially prejudices the Customer's rights or obligations under the Customer Agreement, the Customer may terminate the Customer Agreement by providing written notice to the Company within fourteen (14) days of being notified by Company about the amendment.

(5). Effect of Termination- (i) If the Customer terminates the Customer Agreement pursuant to the preceding paragraph, the termination shall be effective on the date immediately preceding the effective date of the amended Terms or Service Description. (ii) In such event, the Company shall refund to the Customer any pre-paid fees for the Services on a pro-rata basis for the period following the termination date. (iii) If the Customer continues to use the Service after the period of fourteen (14) days indicated in numeral (5) of this section without providing notice of termination, the Customer shall be deemed to have accepted the amended Terms or Service Description.

Article 5 (Notification of Changes)

1. The Customer shall promptly notify the Company of any changes to the information provided in the application for use of the Service.
2. The Company shall not be liable for any disadvantage including loss and damage incurred by the Customer due to the Customer's failure to provide the notification required under the preceding paragraph.

Article 6 (Use of the Service)

1. After the Customer Agreement is formed, the Company shall send the license number and other information necessary for activation of the Service to the Customer's registered address or email address. Subsequently, when the Customer activates the Service, the Company shall send instructions for use of the Service, including the User ID, Password, and the URL of the Service website.
2. The Customer may use the Service in accordance with the methods prescribed by the Company, within the scope of the purpose of the Customer Agreement, etc. and without violating any terms thereof.
3. The Customer may use the Service solely for the purpose of conducting its internal business operations (including, but not limited to, the design and development of products designed and manufactured by the Customer). However, if the Customer needs to permit a third-party contractor to use the Service in the course of conducting the Customer's own internal business operations, the Customer may allow such third party to use the Service, provided that such third party complies with the Customer Agreement, etc., and that the Customer assumes full responsibility for any breach of the obligations under the Customer Agreement, etc. by such third party.
4. The Customer shall use the Service at its own risk and shall assume full responsibility for the

Customer's actions taken through use of the Service (including actions by the Customer, its officers and employees, and its subcontractors and agents) and the consequences thereof, and shall not cause any disadvantage, burden, or damage to the Company. For the avoidance of doubt, the Customer assumes all responsibility for the accuracy, reliability, completeness, usefulness, safety, appropriateness, legality, and certainty of any deliverables, outputs, creations, or other results obtained through use of the Service (collectively, the "**Deliverables**"), and the Company provides no warranties whatsoever in respect thereof.

Article 7 (User IDs, etc.)

1. For the User's use of the Service, the Company shall issue a necessary number of User IDs and Passwords based on the number of licenses purchased by the Customer.
2. The Customer may distribute the User IDs assigned to it to Users, based on the number of licenses purchased. The individuals who receive a User ID from or at the request of Customer shall log in to the Service using the User ID and Password and use the Service.
3. Except as otherwise specified by the Company in writing, the Customer shall not permit any third party except from Users to use the User IDs and Passwords, nor shall it sell, transfer, lend or otherwise dispose of them.
4. The Customer shall be responsible for the use and management of any User IDs and Passwords, and the Company shall not be liable for any errors in use or unauthorized use by third parties. If a User ID and Password are issued via a license card (paper medium) designated by the Company and the User loses, damages, or destroys such license card, the Company will not issue an identical license card. In such event, the Company will invalidate the User ID and Password issued via the lost license card and issue a new license card containing a new User ID and Password. The Company may charge the Customer for the costs associated with such license card reissuance.

Article 8 (Management of Personal data, etc.)

1. Except as stipulated in the Service Description, the Company, acting as a Data Processor under the terms of the Data Processing Agreement ("DPA") between the Customer and the Company, which constitutes an integral part of the Customer Agreement and both parties agree to comply with, shall process personal data obtained from the Customer or personal data contained in the Customer's data (collectively "Personal Data" and within the meaning of the term as per the Data Processing Agreement) solely for the purpose of providing the Service, in accordance with the Customer's documented instructions, and as per the DPA. The Company shall not use Personal Data for any other purpose without the prior written consent of the Customer.

   To the extent the Company acts as a Data Controller for any Personal Data, it shall process such Personal Data in accordance with its Privacy Policy, which governs the Company's use of Personal Data when acting in its capacity as a Data Controller.

2. The Company shall process Personal Data in accordance with the Data Protection Laws (as defined in the DPA).

(1) The Customer, as the Data Controller (as defined in the DPA), shall ensure that all necessary permissions and legal bases for the processing of Personal Data have been obtained and ensured prior to providing such data to the Company. The Customer shall be responsible for ensuring that any Personal Data provided to the Company for processing complies with the Data Protection Laws, and that data subjects have been informed of the processing.

For the avoidance of doubt, when collecting or providing to the Company videos, still images, audio, or other Personal Data concerning the Customer's employees in connection with the use of the Service, the Customer shall be responsible for satisfying the requirements of the Data Protection Laws.

(2) The Customer complies with the applicable Data Protection Laws.

(3) The Customer’s Personal Data does not contain any special categories of personal data or sensitive personal data, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a person’s sex life or sexual orientation.

3. Notwithstanding the above, if any Customer Personal Data contains any special categories of personal data or sensitive personal data (such as health data, racial or ethnic origin, or other categories of sensitive data under the Data Protection Laws), the Customer shall notify the Company in advance and ensure that such processing is explicitly agreed upon in writing by both parties. The Customer is responsible for obtaining valid consent or ensuring that another lawful basis exists for such processing.

4. If a dispute arises with any third party, including the data subject (individual) of such personal data or sensitive personal data, due to the Customer's breach of either of the preceding two paragraphs, the Customer shall resolve such dispute at its own responsibility and expense, and the Company shall bear no responsibility whatsoever.

5. The Company may collect personal information or Personal Data using cookies, referrer information, or similar tracking technologies (e.g., pixel tags, web beacons, etc.), and may use such information in association with data about the Customer and/or Customers. The Company will handle personal data in accordance with applicable Data Protection Laws, ensuring that appropriate notices are provided and, where necessary, consent is obtained for the use of cookies and other tracking technologies. If the Customer disables cookies or other tracking technologies, access to certain features of the Service may be restricted. Communication charges may apply for the transmission of usage history information.

Article 9 (Service Territory)

This article is Intentionally left blank.

Article 10 (Loan of Materials)

1. If the Company deems it necessary for providing the Service, the Company may request the Customer to loan the materials, etc. owned by the Customer regarding its management, business, or technology (the "**Materials**") to the Company, and the Customer shall not refuse such request without reasonable grounds.
2. The Company shall use the Materials with the duty of care of a prudent manager and within the scope of operating the Service and, when applicable, subject to the confidentiality obligations in this Terms of Service.
3. Upon termination of the Service or upon the Customer's request, the Company shall promptly return the Materials to the Customer.

Article 11 (Operation Support)

1. During the Customer's use of the Service, the Company may, when it deems necessary, provide technical support to facilitate the Customer's smooth use of the Service (the "**Operation Support**").
2. The Company may request the Customer to cooperate with various investigations necessary for the Company to provide the Operation Support, such as assessing network conditions, error message status, and configuration settings. In such case, the Customer shall cooperate with such request to the extent possible.
3. If the Company's designated operation support personnel (the "**Support Personnel**") deems it necessary for the Company to provide the Operation Support, the Customer shall permit the Support Personnel to enter the Customer's place of business. In such case, the Customer shall permit the Support Personnel to use the Customer Equipment free of charge.

Article 12 (Scope of Operation Support)

1. The Operation Support does not include responses to faults or other troubles arising in connection with the provision of the Service, except for those caused by the Service Equipment.
2. If it becomes necessary to determine whether a fault or other trouble arising in connection with the provision of the Service is caused by the Service Equipment or by other factors, the Customer shall, at its own responsibility and expense, perform such fault isolation, including inquiries to the manufacturer of the Customer Equipment or other relevant parties.
3. The provision of the Operation Support does not guarantee that all issues with the Service will be resolved, that the Service will operate properly in the Customer's environment, or that lost Customer Data will be recovered. The Customer shall, at its own responsibility and expense, take preventive measures to avoid loss of Customer Data, such as creating backups.
4. The following faults shall be excluded from the scope of the Operation Support:

(1) Faults that cannot be determined to be caused by the Service Equipment;
(2) Faults caused by force majeure events such as cyberattacks, fire, power outages, natural disasters, or similar events;
(3) Faults caused by the Customer's use of the Service in breach of the Customer Agreement, etc.;
(4) Faults caused by external services linked to the Company, such as cloud servers; or
(5) Faults caused by other circumstances that would not occur under normal use conditions.

Article 13 (Outsource of the Service, etc.)

The Company may outsource to the third parties all or part of the operations necessary for providing the Customer with the Service. In such case, the Company shall impose on such subcontractors obligations equivalent to those set forth in the Customer Agreement, etc. with respect to the performance of the subcontracted operations.

Article 14 (Access to and Use of Data)

1. Except as provided in this Article, the Company shall not access, view, use, or disclose or provide to third parties the Customer Data or data generated by the Service without the Customer's prior written consent (including consent in electronic form).
2. Notwithstanding the preceding paragraph, on the provison that the Customer Data and data generated by the Service are processed and aggregated into statistical or technical data that cannot directly identify the Customer or its Users or its confidential information, the Company may use such data free of charge to the extent necessary to achieve the following purposes, and may provide such data to third parties as necessary:
   (1) To provide, operate, and manage the Service;
   (2) To enhance the quality, functionality, and convenience through improvement of the Service;
   (3) To investigate and analyze usage status of the Service (including the number of monthly active Users, usage rates of each function in the Service, and error log analysis);
   (4) To appropriately respond to inquiries from the Users;
   (5) To provide such data to the Company’s group companies or subcontractors to the extent necessary for providing the Service and conducting related operations;
   (6) To develop and provide new services;
   (7) To maintain and operate the Service;
   (8) To address malfunctions, errors, or other troubles with the Service
   (9) For other purposes similar to or closely related to the foregoing purposes.
3. Except as stated in the terms of the EU Data Act Addendum, the Company shall have no obligation to provide the Customer with all or any part of the Customer Data or data generated by the Service.

Article 15 (Service Interruption or Suspension)

1. The Company may interrupt or suspend all or part of the Service without prior notice to or consent of the Customer under any of the following circumstances:
   (1) Urgent maintenance work is required due to malfunction of the Service Equipment;
   (2) The system for providing the Service experiences concentrated load;
   (3) It becomes necessary to ensure the Customer's security;
   (4) Computers, communication lines, or other equipment stop due to an accident;
   (5) Operation of the Service becomes impossible due to force majeure events such as cyberattacks, fire, power outages, natural disasters, or similar events;
   (6) The Company's external services, such as cloud servers, experience troubles, service interruption or suspension, suspension of integration with the Service, specification changes, or other issues; or
   (7) The Customer falls under any of the circumstances set forth in Paragraph 1 of Article 21 (Termination of Customer Agreement by the Company).
2. The Company may temporarily interrupt or suspend provision of the Service upon prior notice to the Customer for the purpose of conducting periodic inspection or applying patches to the Service Equipment.
3. The Company shall not be liable for any loss or damage incurred by the Customer, its officers and employees, or its subcontractors or agents, or other representatives due to the Company's inability to provide the Service for any of the reasons set forth in the preceding paragraphs.

Article 16 (Customer's Responsibilities)

1. The Customer and Customer shall use the Service at its own responsibility and expense after confirming in advance that the content of the Service is suitable for Customer's specific purposes.
2. The Customer shall, at its own responsibility and expense, install or manage the Customer Equipment necessary for using the Service and prepare the Internet connection environment and the Customer Equipment. If the Company conditions the provision of the Service on the installation of equipment with certain performance and capabilities, and the Customer terminates, discontinues, or cancels use of the Service after the installation thereof accordingly, the Company shall not be obliged to accept the return of such designated equipment purchased by the Customer or refund the purchase price thereof.
3. The Service shall be provided as available at the time. The Company makes no warranty whatsoever regarding the Service, including but not limited to its completeness, accuracy, applicability, usefulness, availability, safety, reliability, or certainty. The Company further make no warranty that the Service will be suitable for the Customer's specific purposes. Accordingly, the Customer must confirm at its own responsibility that the Deliverables obtained through use of the Service comply with all safety criteria, safety standards, product standards, environmental standards, and other applicable laws and regulations that the

Customer is required to comply with, and the Company shall bear no responsibility whatsoever in this regard.

5. If the Customer causes damage to any third party due to reasons attributable to the Customer, or receives a claim or other demand from any third party in connection with the Customer's use of the Service, the Customer shall handle and resolve such matter at its own responsibility and expense. The same shall apply if the Customer suffers damage from any third party or makes a claim against any third party in connection with the Customer's use of the Service.
6. The Customer shall implement security measures at its own responsibility and expense, such as preventing computer virus infection, unauthorized access, and information leakage, according to the Customer's environment for using the Service. Except in cases of the Company's willful misconduct or negligence, the Company shall not be liable for any loss or damage incurred by the Customer due to computer virus infection, unauthorized access, or information leakage.
7. The Customer shall back up and store the identical copies of the Customer Data at its own responsibility and expense, and the Company shall bear no responsibility for the storage, preservation, or backup of such data.
8. If the Customer causes damage to the Company in connection with the Customer's use of the Service, the Customer shall compensate the Company for such damage.
9. If a dispute arises in which the Company receives a claim, objection, demand for damage compensation, or any other demand from any third party due to the Customer's use of the Service or the content of data, the Customer shall resolve such dispute at its own responsibility and expense, and the Company shall bear no liability with respect to such dispute. If the Company suffers loss or damage as a result of such dispute, the Customer shall compensate the Company therefor.

Article 17 (Prohibited Acts)

1. The Customer shall not engage in any of the following acts in using the Service:
   (1) Any act that infringes or is likely to infringe intellectual property rights, including patent rights, copyrights, and trademark rights, or other rights of the Company or any third party;
   (2) Any act that unlawfully alters or deletes information stored in the Service Equipment, or falsifies information available for use in connection with the Service;
   (3) Any act that interferes with the Company's operation of the Service;
   (4) Any act of using, or permitting any third party to use, the Service for purposes other than conducting the Customer's internal business operations;
   (5) Any act of providing the Service to any third party in performance of work entrusted to the Customer by such third party;
   (6) Any act that violates applicable laws and regulations or public order and morals;
   (7) Any act that discriminates against or defames the Company or any third party, or damages their honor or credibility;

(8) Any act infringing upon the privacy of a third party;

(9) Criminal acts, acts related to criminal activity, or acts that incite or solicit participation in criminal acts;

(10) Any act of sending unsolicited advertising, promotional, or solicitation emails to any third party, or sending emails that cause or are likely to cause offense to any third party (harassing emails);

(11) Any act that may be detrimental to others, the Company's business, or the Company's reputation, including promoting or disseminating harmful or fraudulent conduct, fraudulent products, services, schemes, or promotions (such as get-rich-quick schemes, pyramid schemes, multi-level marketing, phishing or pharming.), or engaging in other fraudulent conduct;

(12) Any act of using the Service by impersonating any third party;

(13) Any act of unauthorized use of User IDs;

(14) Any act of uploading harmful computer programs such as computer viruses;

(15) Any act that interferes, or is likely to interfere, with the use or operation of any third party's equipment or the Service Equipment:

(16) Any act of using the Service in a manner that compromises the security of networks, computers, communication systems, etc., such as through unauthorized access or interception;

(17) Any act of using networks in an unauthorized manner, such as by circumventing system restrictions;

(18) Any act of using the Service in connection with equipment or devices involving human life, such as medical devices, nuclear facilities or equipment, aerospace equipment, transportation facilities or equipment, weapon systems, or other equipment or devices requiring high reliability, such as submarine repeaters or space satellites;

(19) Any act of uploading information containing specific personal information to the Service, or uploading sensitive personal information to the Service without prior notice to the Company; or

(20) Any other act that the Company deems inappropriate.

2. If the Customer becomes aware of any act falling under any of the items in the preceding paragraph, or believes that such act may occur, the Customer shall immediately notify the Company. The Company shall not be liable for any loss or damage incurred by the Customer as a result of the Customer's engagement in any act falling under any of the items in the preceding paragraph. If the Company incurs any loss or damage as a result of the Customer's engagement in any act falling under any of the items in the preceding paragraph, the Customer shall be obligated to compensate the Company for such loss or damage.

Article 18 (Term of Use)

1. The term of use of the Service shall be one (1) year from the commencement date specified in the Customer Agreement.
2. At least thirty (30) days prior to the expiration of the term of use specified in the preceding paragraph, the Company shall send written or email notice to the Customer, and the Customer shall notify the Company within the specified period whether or not to renew the Customer Agreement.
3. The Company may change the type, content, service fees, and other terms of the Customer Agreement upon renewal of the Service by providing notice of such changes to the Customer at least thirty (30) days prior to the expiration of the term of use.
4. If no application for the next term is confirmed by the expiration date of the current term of use, use of the Service shall be temporarily suspended (password locked) for up to one (1) month from the first day of the following month until an application for the Service is confirmed. If no application for the Service is confirmed by the end of the month following the expiration month, the Customer Agreement shall be terminated and the Customer's account shall be deleted.

Article 19 (Service Fees and Payment Methods)

1. The service fees for the Service shall be as set forth in the Customer Agreement. The Customer shall bear the consumption tax on the service fees and any bank transfer fees or other expenses necessary for the payment thereof.
2. The Customer shall pay the service fees specified in the preceding paragraph in the manner and by the date designated by the Company, in accordance with the invoice issued by the Company, the Authorized Agent, or any other subcontractor of the Company.
3. Even if the Customer is unable to use the Service due to interruption or suspension of the Service as provided in Article 15 (Service Interruption or Suspension) during the term of use, the Customer shall not be exempted from payment of the service fees and other expenses for the term of use, and the service fees and other expenses already paid shall not be refunded, except in the cases where the Customer is unable to use all the functions of the Service for consecutive one (1) month or more due to reasons attributable to the Company. The amount of the refund of the service fees shall be calculated on a monthly basis for the intended term of use of the Service (the period subject to refund shall be rounded down to the nearest month for the purpose of such calculation).
4. In the event of a change in consumption tax during the term of use, the Customer shall settle the monthly prorated amounts of the service fees (for the period from the month in which the tax rate change is applied to the month in which the term of use expires) paid in accordance with the provisions of this Article in the manner prescribed by the Company.

Article 20 (Late Payment Interest)

1. In the event where the Customer delays payment of the service fees and other expenses set forth in the preceding Article (Service Fees and Payment Method) beyond the due date, the Customer shall pay a late fee calculated at a rate of 14.6% per annum on a daily basis, in addition to the amount due.
2. The Customer shall bear bank transfer fees and other expenses necessary for the payment set forth in the preceding paragraph.

Article 21 (Termination of Customer Agreement by the Company)

1. If the Company determines that the Customer falls under any of the following items, the Company may terminate all or part of the Customer Agreement upon notice to the Customer according to the following sub-numerals, and in such case, the Company shall not be liable for any damage incurred by the Customer or any Customer as a consequence of the termination of the Customer Agreement:
   (1) The Customer is in material default or breach of any provision of the Customer Agreement, and despite being notified to remedy such material default or breach by the Company, fails to do so within thirty (30) days of said notice;
   (2) The Customer is subject to compulsory execution, a temporary restraining order for execution, or a petition for an auction;
   (3) A petition is filed by or against the Customer for the institution of proceedings for bankruptcy, civil rehabilitation, corporate reorganization, special liquidation, or other similar proceedings, or the Customer goes into liquidation;
   (4) The Customer fails to pay taxes and dues, and thus receives a demand for payment or is subject to a temporary restraining order;
   (5) The Customer has admitted to its creditors its inability to pay its debts as such debts become due, or any of the promissory notes or checks drawn or endorsed by the Customer has been dishonored;
   (6) There are reasonable grounds to believe that the CustomerCustomer's financial condition has deteriorated or is likely to deteriorate and the Customer is unable to demonstrate the contrary at Company's discretion with documented evidence within a reasonable time determined by Company;
   (7) If the Customer violates Article 17 (Prohibited Acts) and the Customer is unable to demonstrate its non-violation of it at Company's discretion with documented evidence within a reasonable time determined by Company;
   (8) It is considered that the provision of the Service will cause a significant economic or technical burden or a significant security risk to either party;
   (9) It becomes necessary to terminate the Customer Agreement in compliance with the law or a request from a government agency;
   (10) The Company deems the provision of the Service by the Company to be illegal and the

Customer is unable to demonstrate the contrary at Company's discretion with documented evidence within a reasonable time determined by Company; or

(11) The Company otherwise reasonably determines that it is necessary to terminate the Customer Agreement.

2. The Customer shall immediately pay any unpaid service or other fees or liquidated damages for late payment, if any, upon termination of the Customer Agreement under the preceding paragraph.

Article 22 (Discontinuation of the Service)

1. The Company may discontinue all or part of the Service and terminate all or part of the Customer Agreement on the date of discontinuation of the Service under either of the following circumstances:

(1) When the Company has notified the Customer of the discontinuation of the Service at least thirty (30) days prior to the date of discontinuation; or

(2) When the provision of the Service becomes impossible due to force majeure events such as cyberattacks, fire, power outages, natural disasters, or discontinuation or specification changes, etc. of external services linked to the Company such as cloud servers.

2. If the Company discontinues all or part of the Service under the preceding paragraph, the Company shall return to Customer a pro-rata portion of any service fees that have been already paid by Customer for the period that the Customer shall not receive the prepaid services. In cases of discontinuation linked to breaches of the Customer Agreement by Customer, Company shall not refund any service fees to Customer.

Article 23 (Effect of Termination)

1. Upon termination of the Customer Agreement, the Customer shall lose the access rights to the Customer Data (including all or any part of the reproductions thereof; the same shall apply hereinafter) and data generated by the Service. In this case, the Company may delete the Customer Data and data generated by the Service without prior notice and shall have no obligation to authorize the Customer to use such data.

2. Even after the termination of the Customer Agreement, the provisions set forth in Article 14 (Access to and Use of Data), Article 16 (Customer's Responsibilities), Article 24 (Ownership of Rights), Article 25 (Limitation of Liability for Damages), Article 26 (Disclaimer), Article 28 (Confidentiality), and Article 31 (Jurisdiction) shall remain in effect.

Article 24 (Ownership of Rights)

1. Any intellectual property rights, including copyrights, in and to the software, text, images, programs, graphics, and other data that constitute the Service, as well as all other rights therein, belong to the Company or its licensors. The provision of the Service under the Customer Agreement does not grant the Customer any license to use the intellectual property

rights of the Company or its licensors related to the Service, except as expressly set forth in these Terms. The Customer, except for the purpose of using the Service, shall not, without the Company's prior consent, reproduce, copy, republish, transmit, store, sell, publish, or otherwise use such materials in any manner or form.

2. In using the Service, the Customer represents and warrants to the Company the matters set forth in the following items:
   (1) The Customer owns all intellectual property rights and all other rights in the Customer Data, or has obtained licenses from the rights holder to use such Customer Data;
   (2) The Customer Data does not promote or facilitate illegal activities;
   (3) The Customer Data is not detrimental to others, the Company's business, or the Company's reputation, including promoting or disseminating fraudulent products, services, schemes, or promotions (such as get-rich-quick schemes, pyramid schemes, multi-level marketing, phishing or pharming, etc.), or engaging in other fraudulent conduct;
   (4) The Customer Data does not infringe upon any rights of any third party;
   (5) The Customer Data does not infringe upon the privacy of any third party;
   (6) The Customer Data does not contain computer viruses or other harmful contents;
   (7) The Customer Data does not incite or solicit any criminal acts, acts related to criminal activity, or participation in criminal acts; or
   (8) The Customer Data does not relate to military information.
3. Any problem arising from the Customer's violation of the preceding paragraph shall be resolved by the Customer at its own responsibility and expense, and the Company shall not be liable therefor.

Article 25 (Limitation of Liability for Damages)

Regardless of liability for non-conformity, tort, or any other legal cause of action, the scope of liability of the Company to the Customer for damages in connection with the Service or the Customer Agreement. shall be limited to ordinary damage actually incurred by the Customer due to reasons attributable to the Company or as a direct result of the Company's breach of the Customer Agreement, and the amount of compensation for damages shall not exceed the total consideration for the Service paid by the Customer for the last twelve (12) months. In no event shall the Company be liable for any damage arising from reasons not attributable to the Company and any indirect, special, incidental, consequential damages and lost profits (including lost business profits, damages due to business interruption, loss of data, and loss of business information), regardless of whether or not the Company has foreseen such damages or has notified of the possibility of their occurrence. The aforementioned limitations of liability do not apply in cases of mandatory statutory liability (in particular under Product Liability Law) or in the event of gross negligence of Company.

Article 26 (Disclaimer)

1. The Company makes no warranties, whether express or implied, of non-infringement of any right of a third party, fitness for particular purpose and merchantability including legal liability for non-conformity, regarding the content and the provision of the Service.
2. The Company makes no warranties to the Customer of safety, comprehensiveness, reliability, usefulness, completeness, accuracy, applicability, availability, legality, certainty, and suitability for particular purpose or any other performance of the information, etc. provided through the Service (including but not limited to the Deliverables), except otherwise provided in these Terms.
3. The Customer shall prepare the Customer Equipment, etc. necessary for the use of the Service, except otherwise provided in these Terms, and the Customer shall comply with the contract. concerning the use of the Customer Equipment, etc. Furthermore, the Company shall not be liable for any damage incurred by the Customer arising from the Customer Equipment.
4. The Company makes no warranties regarding availability, reliability and safety of the Service even in an environment satisfying the operation guarantee for the Service, and shall not be liable for any damage incurred by the Customer arising from defects, failures or other issues affected by equipment used for the Service, its OS, or other installed software, etc. or malfunctions of equipment used for the Service.
5. The Company shall not be liable to the Customer for data transmission delay, data extraction failures, data upload failures, data download failures, data transmission failures, or data deletion failures, or other failures caused by (i) network delay due to service disruption or network congestion of a telephone company, an internet service provider, or a cloud service provider, (ii) defects in the Service Equipment, etc. or the Customer Equipment, etc., or (iii) force majeure events such as cyberattacks, fire, power outages, natural disasters, or similar events.
6. The Company shall not be liable for any damage incurred by the Customer or any third party, such as leakage or loss of data in connection with the provision, delay, change, interruption, suspension, discontinuation or other troubles of the Service due to the events stipulated in the preceding paragraph.
7. The Customer acknowledges and agrees in advance that the Service shall be used by the Customer jointly with other Customers, that the Customer shall retain and manage the data registered and stored by the Customer at its discretion and responsibility, and that the Company makes no warranty with respect thereto, including without limitation any warranty regarding any damage to, loss of, or leakage of such data, nor is the Company liable for them.

Article 27 (Exclusion of Anti-Social Forces)

1. The Customer represents and warrants the following items;
   (1) The Customer, its employees, its officers, or its shareholders, etc., who substantially own or control the Customer (the "**Customer and its affiliates**") does not or shall not, during

the term of use of the Service, fall under any of the following; an organized crime group, a member of an organized crime group, an associate member of an organized crime group, a person who ceased to be a member of an organized crime group for less than five (5) years, a company affiliated with any organized crime group, a corporate racketeer (*sokaiya*), a social movement racketeer (*shakai undo hyoubo goro*), a political movement racketeer (*seiji katsudo hyoubo goro*), a specialized intellectual crime group (*tokushu chino boryoku shudan*), or any other antisocial group or individual equivalent thereto ("**Anti-Social Forces**".)

(2) The Customer does not fall under a group or an individual who conducts, either directly or through any third party, an act using fraudulent means, a violent demand, or threatening words, an unreasonable demand, obstruction of business, or an act that damages reputation or credit.

2 The Customer represents and warrants that the Customer and its affiliates do not fall under the following items:

(1) Having a relationship where Anti-Social Forces are found to control its management;

(2) Having a relationship where Anti-Social Forces are found to be substantially involved in its management;

(3) Having a relationship where the Customer is found to unduly utilize Anti-Social Forces, such as for the purpose of seeking unjust profits for itself or a third party, or inflicting damage upon a third party;

(4) Having a relationship where the Customer is found to be involved with Anti-Social Forces, by providing funds, etc. or benefits to Anti-Social Forces

(5) Having a close human, capital or economic relationship or a socially reprehensible relationship with Anti-Social Forces, a group or an individual equivalent thereto; or

(6) Having any other relationship similar to any of the preceding items.

Article 28 (Confidentiality)

1. Except as otherwise set forth in these Terms and the Service Description, either the Company or the Customer shall maintain in confidence all technical, business and operation information disclosed by the other party (the "**disclosing party**") for the purpose of performing the Service that has been in advance expressly specified as confidential by the disclosing party (collectively, the "**Confidential Information**"), and shall not divulge such Confidential Information to any third party (excluding the Company's subcontractors and affiliated companies within the Company's group) without the disclosing party's prior written consent. Notwithstanding the foregoing, any information that falls under any of the following items shall not be included in the Confidential Information:

(1) Any information that has been possessed by the recipient of the information (the "**receiving party**") prior to the receipt of the information by the receiving party;

(2) Any information that has been already in the public domain or publicly available at the

time of receipt of the information by the receiving party;

(3) Any information that has become in the public domain or publicly available after receipt of the information by the receiving party due to reasons not attributable to the receiving party;

(4) Any information that the receiving party has lawfully obtained from the duly authorized third party after the receipt of the information without any confidentiality obligations; or

(5) Any information that has been independently developed by the receiving party without use of the Confidential Information.

2. Notwithstanding the preceding paragraph, either the Company or the Customer may disclose Confidential Information without the other party's prior written consent in any of the following cases:

(1) Disclosure in accordance with applicable laws and regulations;

(2) Disclosure is required by an order of any court or other administrative authority;

(3) Disclosure in the course of litigation, arbitration, or other legal proceedings to pursue rights under the Customer Agreement; or

(4) Disclosure to a third party is reasonably required in similar case to the preceding item.

Article 29 (Non-Waiver)

Even if the Company does not exercise any rights set forth in the Customer Agreement, etc., it shall not be deemed to have waived such rights.

Article 30 (Prohibition of Assignment)

The Customer shall not assign, transfer, pledge or otherwise dispose of its status, rights or obligations under the Customer Agreement, etc., in whole or in part, to any third party, without prior written consent of the Company.

Article 31 (Jurisdiction)

Any dispute between the Customer and the Company arising out of or in connection with the Service or any other matters stipulated in the CustomerAgreement. shall be subject to the exclusive jurisdiction of the Osaka District Court in Japan in the first instance.

Article 32 (Governing Law)

The formation, validity, performance, and interpretation of the Customer Agreement, etc. shall be governed by the laws of Japan.

Article 33 (Consultation, etc.)

Any questions concerning matters stipulated in the Customer Agreement, etc. and any matters not stipulated therein shall be resolved through good-faith mutual consultation. Furthermore, if any provision of the Customer Agreement, etc. becomes illegal, invalid or unenforceable in

any respect under the law of any jurisdiction, the validity of the remaining provisions hereof shall not be affected and remain valid enforceable, and the invalid provision shall be replaced by a valid provision that results most close to the intent of such invalid provision.

End of Document

Effective Date: March 23, 2026

ADDENDUM TO CUSTOMER AGREEMENT
EU DATA ACT ADDENDUM

This EU Data Act (Regulation (EU) 2023/2854 ("**Data Act**")) Addendum ("**Addendum**") sets out the terms and conditions for switching requests made by Customer pursuant to and in compliance with the EU Data Act in relation to the Service.

The terms in this Addendum supplement the terms of the Customer Agreement. In the event of a conflict between the terms of this Addendum and the terms of the Customer Agreement or any other document related to the subject matter contained in the Customer Agreement, the terms of this Addendum shall prevail.

Capitalised terms not otherwise defined in this Addendum shall have the meaning set out in the Customer Agreement.

Article 1 (Request process)

1. A Customer that is established or located in the European Union may at any time request ("**Request**") the Company i) to switch to a data processing service (as defined in the Data Act) offered by a different provider of data processing services or to port all exportable data and digital assets (as both defined in the Data Act) to an on-premises ICT infrastructure ("**Switching**") and/or ii) to erase its exportable data and digital assets ("**Erasure**").
2. The Request shall only be processed if it includes all details reasonably necessary for the Company to be able to effectively and efficiently execute it and the Request shall be made with at least two (2) months' notice (the "**Notice Period**").
3. The Customer understands and accepts that submitting a Request will initiate the process that will, subject to the terms of this Addendum, result in the Service no longer being available.

Article 2 (Transition period)

1. The Switching will be completed within thirty (30) days after expiry of the Notice Period, or, if this is technically unfeasible, within an alternative transitional period not exceeding seven (7) months ("**Transition Period**"). The Company shall i) notify the Customer within

fourteen (14) working days after the Customer made the Request if the aforementioned thirty (30) day period is technically unfeasible, ii) duly justify the technical unfeasibility and iii) indicate the specific alternative transitional period.

2. The Customer has a one-time right to, timely, request an extension of the Transition Period.

Article 3 (Switching efforts)

1. During the Transition Period, the Company shall i) provide reasonable assistance to the Customer and third parties authorised by the Customer in relation to the Switching; ii) act with due care to maintain business continuity, and continue the provision of the functions or services under the Customer Agreement; iii) provide clear information concerning known risks to continuity in relation to the Switching and iv) ensure that a high level of security is maintained throughout the Switching.

2. The Company shall also support the (applicable part of) Customer's exit strategy, including by providing all relevant information.

3. The Customer, and all third parties engaged by the Customer, will undertake all reasonable efforts to ensure efficient execution and completion of the Switching, including by performing the timely identification, extraction, exporting, importing and implementing of the exportable data to the applicable destination.

Article 4 (Data export)

1. The Company will allow the Customer to retrieve its applicable data within thirty (30) days after expiry of the Transition Period. Unless Parties agreed differently, subject to the Switching having been completed successfully and to the extent permitted by applicable law, the Company shall erase all exportable data and digital assets generated directly by the Customer, or relating to the Customer directly, after expiry of the aforementioned retrieval period.

2. The Customer will inform the Company of the completion of the data export as soon as possible.

Article 5 (Termination and early termination fees)

1. The Customer Agreement shall be considered to be terminated i) upon the successful completion of the Switching or ii) where Customer's Request concerned erasure of its exportable data and digital assets upon termination of the Service, at the end of the Notice Period.

2. Termination as referred to in Article 5 sub 1 above before expiry of the applicable subscription term for the Service does not entitle the Customer to any refund of the service fees for the Service or of any other payment made by the Customer to the Company under the Customer Agreement. Furthermore, the Company is then entitled to invoice Customer any outstanding fees and expenses and Customer shall pay that invoice – as well as any other unpaid invoices – in accordance with the terms of Article 19 (Service Fees and Payment Methods) of the Terms.

Article 6 (Transition support fees)

1. The costs incurred by the Company that are directly linked to transition support provided before 12 January 2027 (if any) will be charged to the Customer. The Company shall inform the customer in advance about the costs for the specific support needed. Unless Parties agreed otherwise, the Company will invoice those charges after completion of the transition support and the Customer shall pay that invoice, both in accordance with the terms of Article 19 (Service Fees and Payment Methods) of the Terms.

Article 7 (Data and digital assets that can be ported and additional information on switching)

1. The categories of data and digital assets that can be ported during the switching process are published on the designated website for the Service.

2. The categories of data exempted from the exportable data listed in Article 7 sub 1 above are published on the designated website for the Service. These exemptions will not unreasonably impede or delay the Switching.

3. Note that the data, digital assets and exemptions referred to in sub 1 and 2 above may be updated from time to time.

Article 8 (Additional information)

1. Please see the designated website for the Service for more information in relation to Switching and certain international access and transfer.

ADDENDUM TO CUSTOMER AGREEMENT

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**Agreement**") will take effect as of the date on which Customer Agreement was formed in accordance with the Machine Safety Design Hub Terms of Service date ("**Effective Date**")

BETWEEN

OMRON Corporation, a corporation established and existing under the laws of the State of Kyoto, Japan, having its registered office at Kyoto, Japan, at the address Shiokoji Horikawa, Shimogyo-ku, Kyoto 600-8530 Japan, hereinafter referred to as: referred to as: "**Processor**",

and

The Customer with whom the Customer Agreement was formed, in accordance with the Machine Safety Design Hub Terms of Service: "**Controller**",

Collectively, the "**Parties**".

1. BACKGROUND

1.1 Controller and Processor have entered into an agreement (the "**Principal Agreement**") pursuant to which Processor will provide services to Controller ("**Services**") - the usage of Machine Safety Design Hub **("MSDH").**

1.2 Processor enters into this Agreement on behalf of itself and, to the extent required under applicable Data Protection Laws, for the benefit of and on behalf of any entity that is owned or controlled by or is under common control or ownership of Processor and that is (a) subject to Data Protection Laws, and (b) uses the Services pursuant to the Principal Agreement between Controller and Processor ("**Authorised Affiliates**").

As the provision of the Services involves the processing of personal data by Processor, the Parties have agreed to enter into this Agreement for the purposes of ensuring compliance with the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), together with all laws implementing or supplementing the GDPR, the UK Data Protection Laws and any other applicable data protection or privacy laws, including any regulations, guidance, and codes of practice issued by Supervisory Authorities from time to time. UK Data Protection Laws means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("UK GDPR"), together with the Data

Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) and any other data protection or privacy legislation in force from time to time in the United Kingdom **("Data Protection Laws")**. The personal data that is processed by Processor in the course of the Services is defined hereinafter as "**Personal Data**".

2. AUTHORISED AFFILIATES

2.1 Processor enters into this Agreement for itself and, to the extent required under applicable Data Protection Laws, for the benefit of and on behalf of its Authorised Affiliates, where such Authorised Affiliate is considered a data processor for certain Personal Data processed on behalf of Controller. In such case, except where indicated otherwise, the term "Processor" shall include Processor and Authorised Affiliates.

2.2 Processor may invoke the rights and obligations herein on behalf of each Authorised Affiliate and each Authorised Affiliate may invoke such rights and obligations under this Agreement in relation to Personal Data which it is responsible for as data processor as if it were a party.

2.3 Processor that is the contracting party to this Agreement and the Principal Agreement shall remain responsible for coordinating all communication with Controller under this Agreement and is entitled to make and receive any communication or notification in relation to this Agreement on behalf of its Authorised Affiliates.

3. PERSONAL DATA PROCESSING REQUIREMENTS

3.1 Processor and Controller have agreed that Processor shall only process the types of Personal Data relating to the categories of data subjects for the purposes of the Principal Agreement and for the specific purposes in each case set out in Schedule 1 (*Details of the processing of Personal* Data) to this Agreement and shall not process, transfer, modify, amend or alter the Personal Data or disclose or permit the disclosure of the Personal Data to any third party other than in accordance with Controller's documented instructions (whether in the Principal Agreement or otherwise) unless such processing is required by EU or Member State law to which Processor is subject, in which case Processor shall inform Controller of that legal requirement before processing that Personal Data unless the law prohibits this on important grounds of public interest.

4. CONFIDENTIALITY AND SECURITY

4.1 Processor shall ensure that all its employees or other persons that have access to and are involved in the processing of Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.2 Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks in accordance with article 32 GDPR. This includes protecting the Personal Data against a Personal Data Breach. In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

5. SUB-PROCESSING

5.1 Processor has Controller's general authorisation to appoint (and permit each sub-processor appointed in accordance with this section 5 to appoint) sub-processors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 Controller agrees that Processor may continue to use those sub-processors already engaged by Processor as at the Effective data and include in Schedule 2 (*Authorised Transfers of Controller Personal Data*).

5.3 Processor shall give Controller prior written notice of the appointment of any new sub-processor, including full details of the processing to be undertaken by the sub-processor. If within four weeks of receipt of that notice, Controller notifies Processor in writing of any objections to the proposed appointment, Controller shall not appoint the sub-processor.

5.4 Processor shall exercise appropriate care in appointing and overseeing authorized sub-processors and shall enter into contractual terms with authorized sub-processor that impose data protection obligations which are in substance the same as set out in this Agreement. Processor shall remain fully liable to Controller for any failure by a sub-processor to fulfil its obligations in relation to the processing of any Personal Data.

6. DATA SUBJECT RIGHTS

6.1 Processor shall promptly notify Controller if it receives a request from a data subject under any Data Protection Laws in respect of Personal Data, including requests by a data subject to exercise rights in chapter III of GDPR, and shall provide full details of

that request. Processor shall not respond to the request itself unless authorised to do so by Controller in writing.

6.2 Processor shall co-operate and assist as requested by Controller to enable Controller to comply with its obligations to respond to any exercise of rights by a data subject under any Data Protection Laws in respect of Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws in respect of Personal Data or this Agreement, which shall include, as far as this is possible, implementing any additional technical and organisational measures as may be reasonably required by Controller to allow Controller to respond effectively to relevant complaints, communications or requests.

7. DATA BREACHES

7.1 Processor shall without undue delay notify Controller after becoming aware of a data breach involving Personal Data and Processor shall:

7.1.1 immediately take appropriate measures to address the Personal Data breach including measures to mitigate its adverse effects;

7.1.2 provide full assistance and provide Controller with all information which allows Controller to meet any obligations to report a data breach as prescribed by art. 33 and 34 of the GDPR;

7.1.3 further co-operate with Controller and take such steps as are directed by Controller to assist in the investigation, mitigation and remediation of each data breach.

8. ASSISTANCE TO CONTROLLER

8.1 Processor shall provide reasonable assistance to Controller with any data protection impact assessments or with any prior consultations to any Supervisory Authority of Controller which are required under Data Protection Laws, in each case in relation to processing of Personal Data by Processor on behalf of Controller and taking into account the nature of the processing and information available to Processor.

9. INTERNATIONAL TRANSFERS OF CONTROLLER PERSONAL DATA

9.1 Controller permits Processor to process Personal Data in a country outside of the European Economic Area (**"EEA"**), Switzerland, UK or a country that is not an

Adequate Third Country subject to the conditions that the Parties have executed the Module 2 Standard Contractual Clauses (Transfer controller to processor) – as adopted by the European Commission via its implementing decision of 4 June 2021 – and UK IDTA between Controller a data exporter and Processor as a data importer to ensure compliance with obligations related to international transfers in accordance with Chapter V GDPR. These executed Module 2 Standard Contractual Clauses and UK IDTA are attached as Schedule 3 and 4 to this Agreement.

9.2 Processor may (permanently or temporarily) process the personal data or permit any authorised sub-processor to (permanently or temporarily) process the Personal Data in a country outside of the EEA, Switzerland, UK or in a country without an adequate level of protection, provided that the relevant Standard Contractual Clauses and/or UK IDTA are executed.

9.3 If, at any time, a Supervisory Authority or a court with competent jurisdiction over a Party mandates that transfers from controllers in the EEA or UK to processors established outside the EEA or UK must be subject to specific additional safeguards (including but not limited to specific technical and organisational measures), the Parties shall work together in good faith to implement such safeguards and ensure that any transfer of Personal Data is conducted with the benefit of such additional safeguards

10. AUDIT RIGHTS

10.1 Upon Controller's request, Processor shall make available to Controller all information necessary to demonstrate compliance with this Agreement. Processor will deal promptly and adequately with such enquiries. The costs of such audits shall be borne by Controller.

11. DELETION OR RETURN OF CONTROLLER PERSONAL DATA

11.1 Upon the termination or expiration of the Principal Agreement (unless continued processing is subject to a new or amended agreement) and to the extent not prohibited by applicable law, Processor will within 30 days, at the choice of Controller, return or delete the Personal Data.

12. INDEMNITY AND LIABILITY

12.1 Controller warrants that all Personal Data processed by Processor has been and shall be collected and processed by Controller in accordance with any applicable Data Protection Laws.

12.2 Notwithstanding any contrary provisions in the Principal Agreement, Controller indemnifies and holds Processor harmless against all claims, actions, third party or Supervisory Authority claims, losses, damages and expenses incurred by Controller and arising directly or indirectly out of or in connection with a breach of this Agreement by Controller.

12.3 The exclusions and limitations of the liability of Processor set out in the Principal Agreement shall also apply to this Agreement.

13. MISCELLANEOUS

13.1 As of the Effective Date, this Agreement shall automatically replace any existing data processing agreements in place between the Parties in respect of the Services.

13.2 Parties agree that this Agreement and the Standard Contractual Clauses shall terminate automatically upon termination of the Principal Agreement or expiry, or termination of all service contracts entered into by Processor with Controller pursuant to the Principal Agreement, whichever is later.

13.3 With regard to the subject matter of this Agreement, in the event of inconsistencies between the provisions of this Agreement and any other agreements between the Parties, including but not limited to the Principal Agreement, the provisions of this Agreement shall prevail with regard to the Parties' data protection obligations for Personal Data. In the event of any conflict or inconsistency between this Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.4 Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either *(i)* amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, *(ii)* construed in a manner as if the invalid or unenforceable part had never been contained therein.

13.5 This Agreement, including the Standard Contractual Clauses, is governed by the laws of the Netherlands. Any disputes arising out or in connection with this Agreement or

the Standard Contractual Clauses shall be brought exclusively before the competent court of Amsterdam.

This Agreement, including the Schedules, is entered into and becomes a binding part of the Principal Agreement as of the Effective Date. As of the Effective Date, this Agreement shall automatically replace any existing data processing agreements in place between the Parties in respect of the Services.

SCHEDULE 1: DETAILS OF PROCESSING OF PERSONAL DATA

This Schedule 1 includes certain details of the processing of Personal Data as required by Article 28(3) GDPR.

1. Subject matter, duration and purposes of the processing of Personal Data

1a. Subject matter of the processing:

☐ Human Resources (HR)

☐ IT

☐ Marketing

☒ Other (please specify)

As per the Principal Agreement

1b. Duration of the processing:

The duration of the processing of Personal Data by Processor under this Agreement is the period of the Principal Agreement.

1c. *Frequency of the processing*:

The Personal Data will be shared on the following basis during the period of the Principal Agreement:

☐ one-off

☒ *continuous*

☐ *Other (please specify)*

1d. Nature and Purpose of the processing:

The purpose of the processing of Personal Data by Processor under this Agreement is the performance of the services as described in the Principal Agreement, mainly to create and maintain a user account for the provision of the MSDH services.

2. The categories of data subject to whom the Personal Data relates

☐ Employee/contingent workers

☒ Customer data (Individual users of the MSDH services)

☐ Other (please specify)

3. The types of Personal Data to be processed

1. Employees/contingent workers

☐ **Employee data/contingent worker data**, more in particular:

☐ *Personal details* - such as name and first name, address, email address, telephone number or other contact information, degree/title, date of birth, gender, nationality, social security or national insurance number, marital or civil partnership status, domestic partners, dependents, citizenship.

☐ *Emergency contact details* - name and contact details of emergency contacts.

☐ *Financial details* - such as bank account details or other financial characteristics.

☐ *Basic work details* - such as work contact details e.g. corporate email address and telephone number, employee identification number, photograph, details regarding the job function, primary work location, working hours, employment status, and terms and conditions of employment, immigration status, work permit details.

☐ *System and application access data* - information required to access Controller's systems and applications such as email account and system passwords, or device information of e.g. mobile phones or laptops.

☐ *Electronic localisation data* - such as GPS position obtained from track & trace systems that are placed in company vehicles.

☐ *Professional qualifications* - professional certifications, special skills including (driver) licenses, language skills, memberships of committees or other bodies, education history.

☐ *Recruitment or selection data* - any Personal Data contained in CV's, application forms, references, record of interviews or interview notes, and selection and verification records, previous (job) experiences and references.

☐ *Video surveillance footage* - as recorded in buildings by the use of video surveillance equipment (CCTV).

☐ *Remuneration and benefits data* - such as details of payment and benefits package, base salary, bonus, compensation type, long term incentives, company credit card data, tax information, salary reviews.

☐ *Leave data* - such as holiday and family related leave records, retirement eligibility.

☐ *Performance management data* - such as colleague and manager feedback, appraisals, outputs from talent programs and formal and informal performance management processes.

☐ *Training and development data* - such as data relating to training and development needs or trainings received.

☐ *Documentation required under immigration laws* - such as citizenship, details of residency, work permit.

☐ *Psychological data* - for example, personality questionnaires as part of an assessment.

☐ *Disciplinary data* - such as any Personal Data contained in records of allegations, investigation and proceeding records and outcomes, and in the context of whistleblowing.

☐ *Termination data* - such as dates and reasons for leaving, termination agreements and payments, exit interviews and references.

☐ *Special categories of data (sensitive data)* - such as physical or mental health data (e.g. days and reasons of sickness, workplace amendments), racial or ethnic origin, religious or similar beliefs, membership of a trade union, the commission or alleged commission by the employee of any offence; and any proceedings for any offence committed or alleged to have been committed by the employee, the disposal of those proceedings or the sentence of any court in those proceedings, or any other judicial measures such as court seizures or individual traffic fines by using a company vehicle.

☐ *Other data* - please specify.

2. Customers

☒ **Customer data**, more in particular:

☒ *Contact details* - such as name, postal address and other contact details, such as telephone number and e-mail address or any other contact details.

☐ *Personal characteristics* - such as gender or other personal characteristics in order to identify representatives of customers.

☒ *Profession and job title* - including information on the specific (sub) sector the customer operates in.

☐ *Data collected automatically through websites* - such as cookies and other technologies to track website visitors.

☐ *Financial details* - such as bank account details or invoicing details.

☐ *Recording of video footage* - as recorded in buildings by the use of video surveillance equipment (CCTV).

☒ *Information relating to the use of services* - such as which services are used or contracted.

☐ *Pictures* - to identify the customer (representative).

☐ *Communication data* - such as any requests, any complaints and any other customer data that Controller receives when communicating with customers via email, online or via social media.

☐ *Health data* - such as health information collected via a healthcare device application provided by Processor.

☐ *Other data* - please specify.

SCHEDULE 2: AUTHORISED TRANSFERS OF CONTROLLER PERSONAL DATA

Company name of recipient	**Details of the Point of Contact**	**Details of the processing**	**Service location**	**Additional safeguards (only in case of data transfer outside the EEA)**
[*Include full legal name and address of each recipient entity to whom data will be transferred*]	[*Include contact person's name, position and contact details*]	[*Include details of the processing to be undertaken by the entity*]	[*Include the location of where the services will be provided, including those within the EEA and outside of the EEA*]	[*If the recipient is located outside the EEA, specify the additional safeguards that are implemented, e.g. signed Model Clauses]*
Omron Digital Co., Ltd.	Nobuhiro Kawasaki Section Manager, New Business Development Group, Safety Div., Product Business Div. HQ., IAB, OMRON Corporation (nobuhiro.kawasaki@omron.com)	Maintenance	Japan	Intra-Group Data Transfer Agreeement
Amazon Web Services, Inc.	Nobuhiro Kawasaki Section Manager, New Business Development Group, Safety Div., Product	Cloud hosting, data storage, and related processing services	Japan	AWS DATA PROCESSING ADDENDUM

	Business Div. HQ., IAB, OMRON Corporation (nobuhiro.kawasaki@omron.com)	required for operation of the system		

SCHEDULE 3: STANDARD CONTRACTUAL CLAUSES: MODULE 2 TRANSFER FROM CONTROLLER TO PROCESSOR

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

(1) 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

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

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

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

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

Clause 2

Effect and invariability of the clauses

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

Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third party beneficiaries

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

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

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

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

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

(5) Clause 13;

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

(7) Clause 16(e);

(8) 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

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.

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure of return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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:

(a) 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;

(b) 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;

(c) 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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

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

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

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

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

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

sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim

back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

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

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

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

Clause 13

Supervision

(a) 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

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures

authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

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

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

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

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

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under

paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

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

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of

destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

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

SECTION IV– FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

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

(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.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1.	Name:	The Customer, as defined in MSDH ToS
	Address:	The Customer's address, as provided in relation to the Principal Agreement
	Contact person's name, position and contact details:	The Customer's contact details, as set out in the Order Form
	Activities relevant to the data transferred under these Clauses:	As per the Data Processing Agreement and Principal Agreement
	Role (controller/processor):	Controller

Data importer(s):

1.	Name:	**OMRON Corporation**
	Address:	Shiokoji Horikawa, Shimogyo-ku, Kyoto 600-8530 Japan
	Contact person's name, position and contact details:	OMRON Corporation's contact details, as set out in the Order Form
	Activities relevant to the data transferred under these Clauses:	As per the Data Processing Agreement and Principal Agreement
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As described in Schedule 1 part 2 of the Data Processing Agreement

Categories of personal data transferred

As described in Schedule 1 part 3 of the Data Processing Agreement

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.

As described in Schedule 1 part 3 of the Data Processing Agreement

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

As described in Schedule 1 part 1 of the Data Processing Agreement

Nature of the processing

As described in Schedule 1 part 1 of the Data Processing Agreement

Purpose(s) of the data transfer and further processing

As described in Schedule 1 part 1 of the Data Processing Agreement

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

As described in Schedule 1 part 1 of the Data Processing Agreement

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

As described in Schedule 2 of the Data Processing Agreement

C. COMPETENT SUPERVISORY AUTHORITY

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

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*)

ANNEX II

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

The measures Processor has taken include, as appropriate and without limitation:

Category 1 - Access control of persons

Processor shall implement suitable measures in order to prevent unauthorised persons from gaining access to the data processing equipment as long as the personal data transferred by Controller are processed.

This shall be accomplished by:

- Establishing access authorisations for employees and third parties, including the respective documentation;
- Code card passes;
- Restrictions on keys;
- Best practices and guidance for third parties;
- Regulations on key codes;
- Identification of the persons having access authority;
- Security alarm system or other appropriate security measures including after working hours;
- Securing the decentralized data processing equipment and personal computers;
- Protection and restriction of access path; and
- Other measures.

Category 2 - Access control to personal data

Processor commits that the persons entitled to use the data processing system will only be able to access the personal data within the scope and to the extent covered by the respective access permission (authorisation).

This shall be accomplished by:

- Locking of terminals;

- Allocation of individual terminals and/or terminal user and identification characteristics exclusive to specific functions;
- Functional and/or time restricted use of terminals and/or terminal users and identification characteristics;
- Regulations for user authorisation;
- Obligation to comply with confidentiality expectations;
- User codes for personal data and programs;
- Coding routines for files;
- Differentiated access regulations (e.g. partial blocking);
- Regulations for the organisation of files;
- Logging and analysis of use of the files;
- Controlled destruction of data media;
- Work instructions for templates for the registration of personal data;
- Checking, adjustment and controlling systems;
- Processes for the checking and release of programs; and
- Other measures.

Category 3 - User Control

Processor shall implement suitable measures to prevent its data processing systems from being used by unauthorised persons by means of data transmission equipment. In addition, Processor shall implement suitable measures to prevent unauthorised reading, copying, alteration or removal of the data media, unauthorised input into memory, reading, alteration or deletion of the stored personal data.

This shall be accomplished by:

- Authorisation design;
- Terminal with access user key;
- Identification of the terminal and / or the terminal user within the system of the relevant data processor;
- Automatic turn-off of the user ID when several erroneous passwords are entered;
- Log file of events (monitoring of break-in attempts);

- Issuing and safeguarding the identification codes;
- Dedication of individual terminals and/or terminal users;
- Identification characteristics exclusive to specific functions;
- Authentication of the authorised personnel;
- Protective measures for the data input into memory as well as for the reading, blocking and deletion of stored personal data;
- Use of encryption for critical security files;
- Specific access rules for procedures, control cards, process control methods, program cataloguing authorisation;
- Guidelines for data file organisation;
- Keeping records of data file use;
- Separation of production and test environments for libraries and data files;
- Providing that entries to data processing facilities (rooms, housing, computer hardware and related equipment) are capable of being locked;
- Automatic log-off of user IDs that have not been used for a substantial period of time;
- Designating the areas in which data media may / must be located;
- Designating the persons in such areas for authorised removal of data media;
- Controlling the removal of data media;
- Securing the areas in which data media are located;
- Release of data media only to authorised persons;
- Control of files, controlled and documented destruction of data media;
- Policies controlling the production of backup copies; and
- Other measures.

Category 4 - Transmission control

Processor shall be obliged to enable the verification and tracing of the locations/destinations to which the data subject's personal data are transferred by the utilization of Processor's data communication equipment/devices.

This shall be accomplished by:

- Authentication of the authorised personnel;

- In-house verification requirements (four-eye principle);
- Designating the areas in which data media may / must be located;
- Controlling the removal of data media;
- Designating the persons in such areas who are authorised to remove data media;
- Control of files;
- Locking of confidential data media;
- Security lockers;
- Prohibition of taking bags etc. within the secure area;
- Control of destruction of data media;
- Policies controlling the production of backup copies;
- Documentation of the transfer programs;
- Documentation of the retrieval and transmission programs;
- Documentation of the remote locations/destinations to which a transmission is intended and the transmissions path (logical path);
- Authorisation policy;
- Encryption of the data for online transmission or transport by means of data carriers (tapes and cartridges);
- Monitoring of the completeness and correctness of the transfer of data (end to end check);
- Encryption;
- Courier services, personal pickup, accomplishing of the transport;
- Control of plausibility;
- Control of completeness and correctness;
- Deletion of remaining personal data before change of data media; and
- Other measures.

Category 5 - Input Control

Processor shall provide for the retroactive ability to review and determine the time and the point of the data subject's personal data entry into Processor's data processing system.

This shall be accomplished by:

- Proof of relevant data processor's organisation of the input authorisation;
- Electronic recording of entries;
- Electronic recording of data processing, in particular usage of data; and
- Other measures.

Category 6 - Organisation Control

Processor shall maintain its internal organisation in a manner that meets the requirements of this Agreement.

This shall be accomplished by:

- Internal data processing policies and procedures, guidelines, work instructions, process descriptions and regulations for programming, testing and release, insofar as they relate to the personal data transferred by the data controller;
- Formulation of a data security concept;
- Industry standard system and program examination;
- Formulation of an emergency plan (backup contingency plan); and
- Other measures.

Category 7 - Instructional Control

The data transferred by Controller to Processor may only be processed in accordance with the instructions of Controller.

This shall be accomplished by:

- Policies and procedures for Processor's employees;
- Upon request, access will be granted to those of Controller's employees and agents who are responsible for monitoring Processor's compliance with this Agreement; and
- Other measures.

Category 8 - Control of Separation of Personal Data

Processor shall implement suitable measures to allow the separate processing of personal data that has been collected for different purposes.

This shall be accomplished by:

- Storage of the personal data in separated data collectors (physical separation);
- Authorisation policy (logical separation); and

- Separation of the personal data, which have been stored under an alias (pseudonym) from the original personal data.

ANNEX III

LIST OF SUB-PROCESSORS

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

As described in Schedule 2 of the Data Processing Agreement.

SCHEDULE 4: UK STANDARD CONTRACTUAL CLAUSES – UK ADDENDUM: MODULE 2 TRANSFER FROM CONTROLLER TO PROCESSOR

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

Part 1: Tables

Table 1: Parties

Start date	As per the Data Processing Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: The Customer, as defined in MSDH ToS Trading name (if different): N/A Main address (if a company registered address): The Customer's address, as set out in the Order Form Official registration number (if any) (company number or similar identifier): As set out in the Order Form	Full legal name: OMRON Corporation Trading name (if different): N/A Main address (if a company registered address): Shiokoji Horikawa, Shimogyo-ku, Kyoto 600-8530 Japan Official registration number (if any) (company number or similar identifier): As set out in the Order Form
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Reference (if any): *Included in Schedule 4 of the Data Processing Agreement* 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	x	*	*	*	*	
3						
4						

*as set out in the EU Standard Contractual Clauses contained at Schedule 4 of the Data Processing Agreement.

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: *As described in the Data Processing Agreement*
Annex 1B: Description of Transfer: *As described in Schedule 1 of the Data Processing Agreement*
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: *As described in Schedule 3 of the Data Processing Agreement*
Annex III: List of Sub processors (Modules 2 and 3 only): *As described in Schedule 2 of the Data Processing Agreement*

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 ☒ neither Party

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

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.